VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Petr Košina

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

VYUŽITÍ FYZICKY NEKLONOVATELNÝCH FUNKCÍ V KRYPTOSYSTÉMECH
USE OF PHYSICALLY UNCLONABLE FUNCTIONS IN CRYPTOSYSTEMS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Petr Košina**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Václav Zeman, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Petr Košina ***ID:*** 203262
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Využití fyzicky neklonovatelných funkcí v kryptosystémech

POKYNY PRO VYPRACOVÁNÍ:

Práce se bude zabývat rozborem vlastností fyzicky neklonovatelných funkcí (FNF) a vhodnosti jejich využití v kryptosystémech. Na základě zvolených kritérií proveďte klasifikaci jednotlivých typů FNF. Identifikujte a popište vhodné FNF pro implementaci v méně výkonných elektronických zařízeních. Navrhněte a realizujte softwarový systém, který bude demonstrovat využití FNF pro autentizaci.

DOPORUČENÁ LITERATURA:

[1] BÖHM, Christoph a HOFER, Maximilian. Physical unclonable functions in theory and practice. Springer Science & Business Media, 2012.

[2] PAPPU, Ravikanth. Physical one-way functions. 2001. PhD Thesis. Massachusetts Institute of Technology.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

Abstrakt

Předmětem bakalářské práce je seznámení s problematikou fyzicky neklonovatelných funkcí, výčet a komparativní analýza jejich jednotlivých druhů. Výstupem tohoto porovnání je pak seznam ideálních kandidátů pro případný vývoj kryptosystému zaměřeného na autentizaci zařízení. V druhé části práce pojednává o vývoji softwarové autentizační aplikace využívající princip FNF. K vývoji samotné aplikace je využito programovacího jazyka python a několika jeho externích knihoven.

Klíčová slova

fyzicky neklonovatelné funkce, FNF, kryptosystém, autentizace, lehká kryptografie, softwarová aplikace

Abstract

The subject of the bachelor's thesis is acquaintance with the topic of Physical Unclonable Functions, enumeration and comparative analysis of their individual species.The output of this comparison is a list of ideal candidates for the possible development of a cryptosystem focused on device authentication.The second part of thesis deals with the development of a software authentication application using the PUF principle.The Python programming language and several of its external libraries are used to develop the application itself.

Keywords

physical unclonable functions, PUF, cryptosystem, authentication, lightweight cryptography, software aplication

Bibliografická citace

KOŠINA, Petr. *Využití fyzicky neklonovatelných funkcí v kryptosystémech* [online]. Brno, 2021 [cit.2021-05-29]. Dostupné z: https://www.vutbr.cz/studenti/zav-race/detail/125895. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Václav Zeman.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	*Petr Košina*
VUT ID studenta:	*203262*
Typ práce:	*Bakalářská práce*
Akademický rok:	*2020/21*
Téma závěrečné práce:	*Využití fyzicky neklonovatelných funkcí v kryptosystémech*

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brně dne: 31. května 2021 ----------

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D. za pedagogickou i odbornou pomoc a další cenné rady při zpracování mé diplomové práce.

V Brně dne: 31. května 2021 ----------

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Fyzicky neklonovatelné funkce (dále také FNF) jsou vlastnosti nejen elektronických zařízení, využívající nesourodostí a výkyvů vzniklých během výrobního procesu k vytváření jedinečných výstupů pro daná zařízení. Lze tak FNF přirovnat například k biometrickému otisku prstu jednotlivých aparátů. Díky tomu představují zajímavou možnost využití, jako rozšíření běžným kryptosystémům, v čemž tkví jejich potenciál do budoucna.

V základu jsou fyzicky neklonovatelné funkce fyzickým systémem generující v závislosti na vstupním signálu (tzv. výzvě), který je pro všechna zařízení identický, signál výstupní (tzv. odpověď), jež je unikátní určitému zařízení. Primárními atributy FNF jsou jedinečnost individuálních mechanismů jimi disponujícími (reprezentována specifickým výstupem) a vysokou obtížnosti nápodoby chování FNF, tedy neklonovatelností. Podrobněji jsou tyto i jiné vlastnosti FNF rozepsány v kapitole 1.3.

Oblastí s největším potenciálem pro využití fyzicky neklonovatelných funkcí se v dnešní době stává obor tzv. „internetu věci“ neboli „Internet of Things“ (IoT). Zde představují FNF formu spolehlivého zabezpečení s nutností vynaložení relativně nízkých nákladů. IoT je zejména reprezentováno nízkonákladovými zařízeními, tedy mechanismy s relativně nízkými napěťovými, paměťovými a výpočetními nároky. Kvůli těmto limitům je pro taková zařízení nevhodné využití klasické, často výpočetně velice náročné, kryptografie vyžadující existenci tajného klíče uloženého v nevolatilní paměti zařízení. Příkladem takových zařízení mohou být mechanismy využívající technologii Arduino, či Raspberry, ale také různá bezpečnostní čidla, RFID čipy a jiné.

Přesto však existují i druhy FNF, které je vhodné použít, jako součást komplexnějších kryptosystémů. V takových případech je zejména apelováno na nenapodobitelnost vnitřních procesů FNF zařízení utvářející výslednou odpověď.

Cílem této práce je provést ucelené pojednání, které pomůže čtenáři se zorientovat v problematice fyzicky neklonovatelných funkcí, dále pak vyhotovit rešerši různých typů FNF a jejich analýzu určující vhodnost využití FNF v kryptosystémech zabezpečující nízkonákladová zařízení. Na závěr se zde objeví návrh a popis realizace softwarového systému demonstrující využití FNF pro autentizaci.

Samotná bakalářská práce je členěna na celkem pět kapitol od kapitoly pojednávající o vlastnostech fyzicky neklonovatelných funkcí, přes jejich stručný výčet a nastínění jejich využití v rámci kryptografie až po návrh a popis činnosti autentizačního systému.

V první kapitole bude čtenář seznámen s historií výzkumu, dále pak s principem činnosti a vlastnostmi, které FNF definují. V závěru kapitoly je krátké pojednání shrnující výhody a nevýhody fyzicky neklonovatelných funkcí.

Druhá kapitola je zaměřena na výčet různých druhů FNF seřazených podle jejich vlastností. Nalezneme zde například zástupce fyzicky neklonovatelných funkcí neelektrických, ale i analogových, či paměťových.

Kapitola třetí je zaměřena na komparativní analýzu vybraných druhů FNF představených v předchozím oddílu. Na závěr této části je v návaznosti na provedenou analýzu vybráno několik málo vhodných kandidátů, které by bylo možné použít pro fyzický návrh instance FNF.

Čtvrtý oddíl je podrobněji věnován potenciálu využiti fyzicky neklonovatelných funkcí v rámci kryptografie. Jedná se konkrétně o užití k autentizaci, generování šifrovacích klíčů a identifikaci.

Finální, pátá část této bakalářské práce je věnována návrhu a samotné tvorbě softwarového řešení autentizačního systému využívající FNF. Sám o sobě je rozdělen na čtyři kategorie věnující se návrhu funkce simulující činnost FNF, inicializačnímu kroku předcházející autentizaci, autentizaci ze strany řídící jednotky a ověření ze strany samotného FNF zařízení.

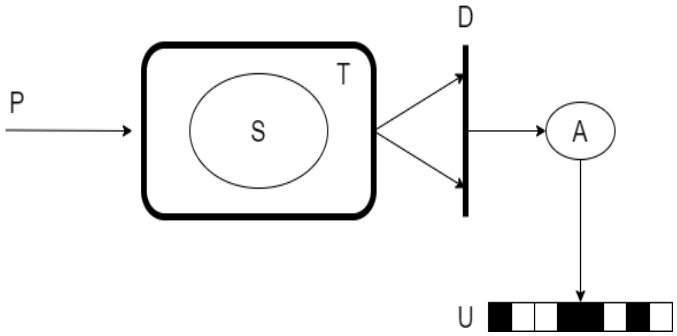
1 Fyzicky neklonovatelné funkce

V první kapitole je stručně vysvětlen pojem FNF, nastíněn vznik a postupný historický vývoj těchto funkcí, dále pak princip činnosti, včetně získávání odpovědi, následné využití vzdálenostních metrik pro vyhodnocení odezvy a aplikace protichybových kódů. Následným a zřejmě nejdůležitějším bodem první kapitoly je popis jednotlivých vlastností, které musí zařízení splňovat, abychom o něm mohli mluvit, jako o zařízení disponujícím FNF. Na závěr kapitoly je pak stručné pojednání o výhodách a nevýhodách fyzicky neklonovatelných funkcí.

Jak již bylo v úvodu naznačeno, fyzicky neklonovatelné funkce jsou funkce s vnitřní nahodilou povahou. Můžeme o nich tedy mluvit, jako o jakémsi hardwarovém otisk zařízení, jež je ekvivalentem lidskému otisku prstu – každé zařízení generuje unikátní nepředvídatelnou odpověď na počáteční výzvu. Právě této rozdílnosti je možno využít k identifikaci, autentizaci, či generování náhodných klíčů pro kryptografické algoritmy. Ačkoliv se nejedná o neznámou oblast na poli zabezpečení informačních systémů, touto problematikou se zabývají odborníci již bezmála 20 let, jedná se o jedno z nejmladších témat v odvětví, což je hlavním důvodem pro místy nesjednocenou anglickou terminologie a téměř neexistujícího českého názvosloví. Z toho důvodu přejímá odborná komunita pro tuto problematiku anglické výrazy.

1.1 Stručný vývoj fyzicky neklonovatelných funkcí

Třebaže myšlenkou využití neklonovatelných vlastností elektrotechnických zařízení se vědečtí pracovníci zabývali již v druhé polovině 20. století (konkrétně D.W. Bauder roku 1983 [1]), byly fyzicky neklonovatelné funkce poprvé jednolitě prezentovány až v roce 2001 doktorem S.R. Pappuem v jeho disertační práci *Physical one-way functions* [19]. S.R. Pappu v tomto díle sestavil ucelený koncept FNF a mimo jiné stanovil čtyři kategorie, obsahující deset primárních kritérií fyzické autentizace, jež by měly fyzicky neklonovatelné funkce splňovat.



Obrázek 1.1 Koncepce autentizačního systému.

Obecný systém fyzické autentizace (graficky znázorněn na obrázku 1.1) se skládá z fyzického systému *S* zapouzdřeného v odpovědi *T*. Fyzická sonda *P* a detektor *D* dohromady vytvářejí čtečku. Sonda *P* působí na systém *S* a vytváří výstup, který je zaznamenán detektorem *D*. Poté algoritmus *A* zpracuje přijatý signál *S* a vytváří jedinečný identifikátor *U*.

Požadavky na fyzický systém

- Vyrobitelnost (easy to fabricate) – „Výroba prototypu fyzického systému musí být snadná a nepříliš finančně náročná."
- Měřitelnost (easy to probe) – „Musí existovat snadný způsob nastavení měřicí sondy pro získání odezvy fyzického systému."
- Nenapodobitelnost (hard to clone) – „Je obtížné vyrobit zařízení, které vyprodukuje jistou odpověď a vzápětí vytvoří jinou odpověď s těmi samými strukturálními vlastnostmi."
- Stabilita (structurally stable) – „Mechanické a elektromagnetické vlastnosti jednotlivých systémů musí být dlouhodobě stabilní."

Požadavky na měřicí sondu

- Snadná vytvořitelnost (easy to generate) – „Systém musí být schopen komunikovat se sondou, která musí být jednoduše a levně vytvořitelná."
- Snadná opakovatelnost specifického stavu (easy to reproduce a specific state) – „Měřicí sonda musí být schopna provést ty samé dotazy, bez ohledu na konkrétní stanici čtečky."

Požadavky na detektor

- Identická odpověď detektoru (identical response) – „Jelikož každá stanice čtečky obsahuje detektor, požadujeme, aby detektor měl identickou odpověď pro identický vstupní požadavek."

Požadavky na vzájemné působení systému a sondy

- Neproveditelnost simulace (impractical or infeasible to simulate) – „Vzájemné působení sondy a systému musí být výpočetně nepraktické a nelze jej simulovat."
- Vysoká citlivost sondy, či systému na změny (output very sensitive to changes in the system or the probe) – „Je požadována vysoká citlivost sondy, což vytváří odolnost proti neoprávněné manipulaci. Veškeré změny v systému jsou snadno detekovatelné."
- Obtížné invertování výstupu (hard to invert) – „Je požadována složitost zjistitelnosti vstupní konfigurace při znalosti výstupu."

Roku 2002 uveřejnil B. Gassend svou disertační práci s názvem: „Silicon physical random function"[6], kde prezentoval své pojetí FNF, jak název díla napovídá Physical

random function – PRF. Jelikož však zkratka tohoto znění byla již v kryptografii zavedena pro pojem pseudonáhodné funkce, ujal se jiný název, který Gassend rovněž ve své práci hojně používá, a to Physical unclonable function, tedy zkráceně PUF. V Gassendově disertační práci lze pozorovat jisté shodné prvky s prací S.R. Pappuho, avšak autor sám přikládá větší váhu vlastnostem vyhodnotitelnost a nepředvídatelnost (*easy to evaluate* a *hard to charakterize*).

Pod tímto termínem byly fyzicky neklonovatelné funkce známy až do roku 2012, kdy svou disertační práci vydal Maes[18], kde jej upravuje na, dnes již pevně zavedený a známý pojem, Physically uncloneable function (z tohoto označení vychází i český překlad). Autor ve svém díle dále poukazuje na fakt, že z matematického hlediska se jedná spíše o funkce pravděpodobnostní. Toto tvrzení zakládá na skutečnosti, že jako odezvu na jeden dotaz může FNF vygenerovat více různých odpovědí. Z toho důvodu je vhodnější o FNF přemýšlet, jako o pravděpodobnostní. Vedle těchto změn Maes upravuje výčet vlastností, které musí FNF splňovat (více v kapitole 1.3).

1.2 Koncept a princip fyzicky neklonovatelných funkcí

1.2.1 Koncept fyzicky neklonovatelných funkcí

Koncept FNF vychází z přirozené unikátnosti každého integrovaného obvodu – instance FNF. Tato jedinečnost spočívá v drobných nesrovnalostech vznikajících v průběhu výroby (intrinzické neboli vnitřní FNF) nebo aplikací vedlejších složek (neintrinzické FNF). Právě tyto odlišnosti jsou příčinou vzniku jedinečného výstupního signálu pro každé jedno zařízení vyvolaného identickým signálem na jejich vstupu. Tzn., že na signál, který přichází na vstup každého aparátu, bude reagováno odlišně. Zároveň je možné výstupní hodnotu duplikovat, což umožňuje zařízení identifikovat.

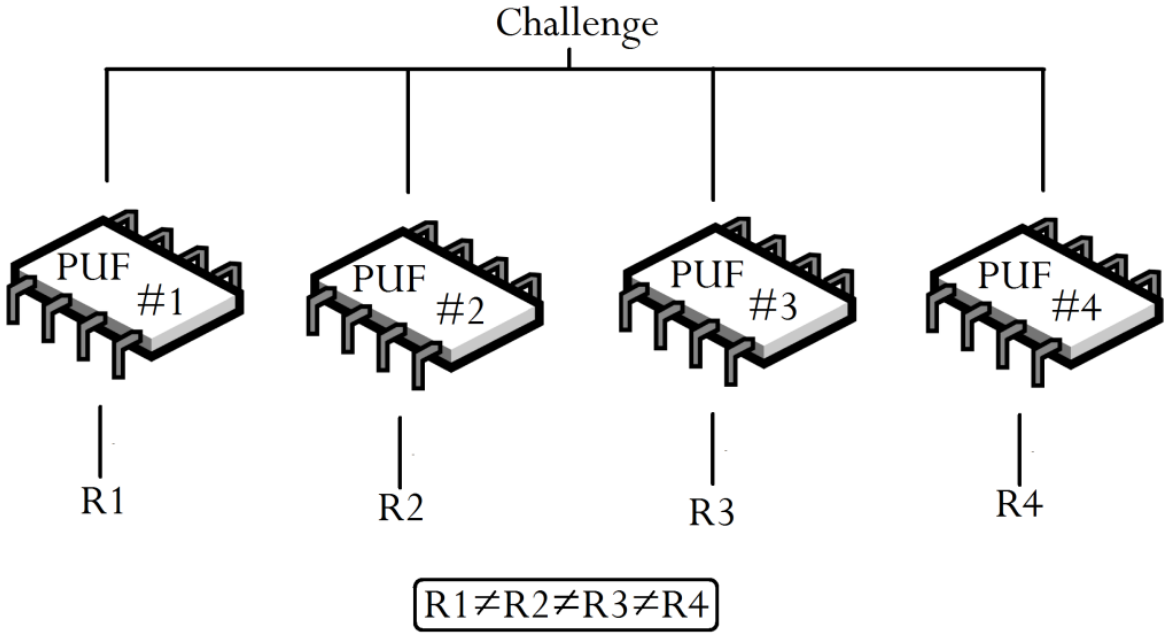
Vnitřní odlišnosti zařízení vzniklé při výrobě nelze předpovědět a zároveň by bylo velice náročné simulovat přesné podmínky, za kterých byl daný komponent vyroben. V závislosti na těchto faktech můžeme s jistotou říct, že každý aparát označující se, jako FNF je unikátní a neklonovatelný.

K samotnému využití fyzicky neklonovatelných funkcí se používá dvojic výzva – odpověď. Ovšem odpovědi na opakovaný shodný dotaz nemusejí být nutně totožné (právě na tuto skutečnost poukázal ve své práci Maes [18]). K získání spolehlivé odpovědi je tedy zapotřebí implementovat na naměřené hodnoty metodu vzdálenostních metrik (problematika vzdálenostních metrik je podrobněji rozebrána v podkapitole 1.2.3). Déle pro stabilizaci získaných hodnot je zapotřebí uplatnit na všechny výzvy směřující na zařízení, ale i příchozí odpovědi tzv. protichybové kódy (více o protichybových kódech v kapitole 1.2.4).

1.2.2 Princip fyzicky neklonovatelných funkcí

Na vstupní port zařízení disponujícího fyzicky neklonovatelnou funkcí je přiveden počáteční signál (jinak známý, jako výzva), na který FNF atribut vzápětí reaguje. Jak již bylo uvedeno výše, zařízení s FNF je, v důsledku vnitřní nestability (vzniklé při výrobním procesu) zdrojem náhodnosti. Zásluhou toho je reakce na vstupní signál (odpověď) jedinečná. Tato odpověď mívá většinou binární podobu [2].

Za předpokladu, že nasměrujeme totožný signál na dvě a více identických zařízení podporující FNF, můžeme v jejich odpovědích zpozorovat rozdílnosti. Výzva, implementována na příslušný FNF orgán, utváří s nově vzniklou odpovědí daného atributu pevně svázanou dvojici výzva – odpověď.



Obrázek 1.2 Princip získání a demonstrace unikátnosti párů výzva – odpověď.

Podobně, jako v případě neuronových sítí i využívání hodnot fyzicky neklonovatelných funkcí předchází tzv. inicializační neboli učící fáze (*enrollment phase*), kdy se vytváří párové spojení výzva – odpověď. Takto nabyté hodnoty se posléze ukládají do databáze párů, kde určité vstupní hodnotě (výzva) odpovídá individuální výstupní hodnota (odpověď) pro jednotlivá zařízení. S tímto postupem přišli roku 2010 Maes se svou kolegyní Ingrid Verbauwhede, který posléze uveřejnili ve svém článku [17]. Při ověřovací fázi (*verification phase*) jsou databázové výzvy opětovně implementovány na FNF atributy, následně se získané odpovědi porovnají s hodnotami získanými dříve. S ohledem na vnitřní nestabilitu FNF systému, může dojít k případu, že nově nabyté odpovědi nebudou zcela dokonale odpovídat hodnotám nabytých při inicializačním kroku. Právě o tuto skutečnost se opírají Böhm a Hofer ve své definici fyzicky

neklonovatelných funkcí: *„FNF je fyzickou entitou, která generuje výstupní hodnotu při nejmenším v závislosti na fyzické struktuře a je obtížně klonovatelnou.“* [2].

1.2.3 Vzdálenostní metriky

Vzdálenostní metriky jsou uplatněny z důvodu nekonzistentnosti odpovědí instance FNF na opakované předložení totožného dotazu. Jelikož si jsou získaná data v podobě odpovědí blízká, je zapotřebí tuto podobnost kvantifikovat. Tato kvantifikace je zprostředkována pomocí tzv. vzdálenostních metrik. Pod tímto názvem se skrývají dva sobě velmi blízké pojmy: inter-vzdálenost (*inter-distance*) a intra-vzdálenost (*intra-distance*).

Inter-vzdálenost lze formulovat jako vzdálenost mezi odpověďmi dvou různých FNF zařízení na stejnou výzvu určující unikátnost odpovědi. Tedy určuje, jak velká je rozdílnost dvou fyzicky neklonovatelných funkcí na základě odlišnosti výsledných odpovědí. Ideální vzdálenost mezi jednotlivými odpověďmi je cca 50 % [17].

Intra-vzdálenost znázorňuje, na rozdíl od inter-vzdálenosti, různorodost výsledných odpovědí pouze jediného FNF na totožnou výzvu, ta je však na zařízení zaslána dvakrát. Líčí tedy průměrnou reprodukovatelnost znovu nabyté odpovědi v porovnání s původním vzorkem. V ideálním případě by měla být intra-vzdálenost rovna nule. [17].

1.2.4 Protichybové kódy

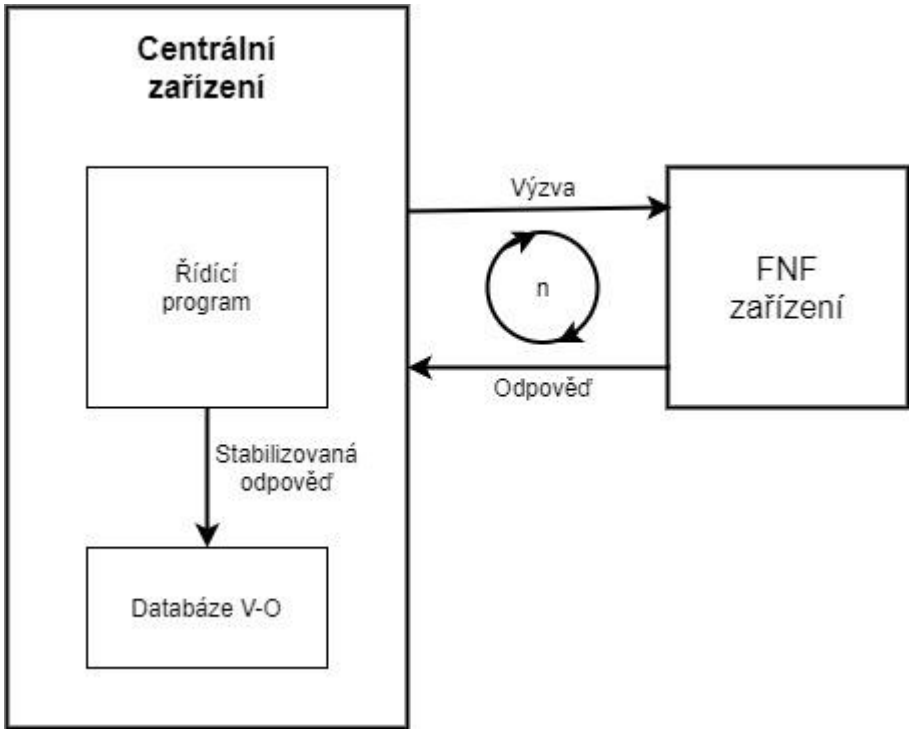
Ačkoliv požadujeme u zařízení FNF, pokud možno co největší entropii odpovědí, může se nakonec stát, že bude dotyčná vlastnost ve výsledku na obtíž. V některých extrémních případech může neurčitost výsledných dat docílit až takové úrovně, že porovnávané odpovědi, vzniklé zasláním identické výzvy, nebudou vyhodnoceny dle vzdálenostních metrik, jako vyhovující [25]. Vedle odlišných podmínek výroby i proměnlivé vlivy okolí, či stárnutí zařízení může způsobovat rozdílnost v odpovědích [13].

Chyby lze dělit z hlediska jejich zdroje na deterministické a nahodilé. Chyby deterministické mají za následek okolní vlivy, jako jsou například teplotní rozdíly, či vlhkost působící na zdroj unikátních instancí FNF. Na druhou stranu náhodné chyby jsou zapříčiněny šumem vlastního obvodu [4].

Jelikož chybovost FNF v proměnlivých podmínkách dosahuje až 25 % je ustálení odpovědi řešeno pomocí protichybových kódů. S návrhem užití těchto algoritmů pro fyzicky neklonovatelné funkce přišel roku 2003 Gassend [7].

Nejjednodušším a zároveň kvalitním typem protichybového kódu je užití tzv. výpočtu střední hodnoty nebo také aritmetického průměru jednotlivých odpovědí. Centrální zařízení si v tomto případě opakovaně (vzhledem k obvykle dvoustavovému charakteru odpovědí je vhodné volit lichý počet opakování) vyžádá od FNF zařízení pro určitou výzvu odpověď, kterou vzájemně sčítá. Po ukončení cyklu shromažďování

odpovědí vydělí řídící program centrálního zařízení celkový součet všech odpovědí počtem opakování. Výsledná hodnota je poté uložena do databáze výzva – odpověď, jako referenční.



Obrázek 1.3 Aplikace samoopravného kódu při učící fázi (n reprezentuje počet opakování).

1.3 Vlastnosti fyzicky neklonovatelných funkcí

Primární vlastnosti FNF vycházejí z návrhu, který prezentoval Pappu [19]. V této kapitole jsou znázorněny vlastnosti fyzicky neklonovatelných funkcí, které stanovil Maes [18] a které se i dnes berou, jako platné. Jedná se šestici definujících charakteristik, které má každé zařízení splňovat, konkrétně to jsou: konstruovatelnost, vyhodnotitelnost, opakovatelnost, jedinečnost, identifikovatelnost a fyzickou neklonovatelnost. Dále pak definoval vlastnosti, jejichž přítomnost je u FNF žádoucí, nikoli však vyžadována (zpravidla se však u FNF vždy vyskytují). Takovými pravidly jsou: nepředvídatelnost, matematickou neklonovatelnost, jednosměrnost a detekovatelnost manipulace.

1.3.1 Konstruovatelnost a vyhodnotitelnost

Jelikož konstruovatelnost podmiňuje samotnou existenci jakéhokoliv zařízení, jedná se o základní a nejdůležitější vlastnost FNF, neboť jsou od ní podmíněny všechny následující vlastnost FNF. Maes vyrobitelnost definuje jako: *„FNF je konstruovatelné, jestliže je jednoduché vytvořit zařízení a vyvolat náhodnou FNF instanci.“* [18]. Ohledně složitosti konstruovatelnosti Maes míní, že je relativní kontextu. Z praktičtějšího hlediska je složitostí rozuměn důraz na výrobní náklady instance konkrétní třídy PUF [18].

S ohledem na to, že všechny následující vlastnosti se zabývají vztahem výzva – odpověď, přikládá Maes vyhodnotitelnosti rovnocený důraz, jako konstruovatelnosti. Autor vyhodnotitelnost definuje jako: „*FNF vykazuje vyhodnotitelnost, jestliže je zkonstruovatelná a pokud jakékoliv náhodné výzvě je přiřazena její odpověď“* [18].

1.3.2 Opakovatelnost

Opakovatelnost nebo také reprodukovatelnost je vlastností zabývající se vztahem mezi párem výzva – odpověď. Reprodukovatelnost přímo souvisí s vzdálenostními metrikami. *„FNF vykazuje opakovatelnost, jestliže je vyhodnotitelná a pravděpodobnost malé intra-vzdálenosti je vysoká.“* [18] Tedy fyzicky neklonovatelná funkce je opakovatelná, když je intra-vzdálenosti mezi odpověďmi reagujícími na jednu výzvu nízká. Pojem „nízká“ intra-vzdálenost je však silně individuální v závislosti na typu FNF, požadavků pro danou aplikaci a preferencích samotného autora instance.

1.3.3 Jedinečnost a identifikovatelnost

Maes definuje jedinečnost, jako: *„FNF je unikátní, jestliže je vyhodnotitelná a pravděpodobnost velké inter-vzdálenosti je vysoká.“* [18] Tedy čím rozdílnějším jsou odpovědi různých výzev mezi sebou, tím jednoznačnější je tvrzení, že FNF splňuje podmínky jedinečnosti.

Identifikovatelností je myšlena vlastnost, že dle odpovědi na totožnou výzvu je možné určit od kterého zařízení byla získána. Dle Maese *„FNF vykazuje identifikovatelnost, jestliže je reprodukovatelná a unikátní, a zvláště jestliže je vysoká pravděpodobnost vztahu inter-vzdálenost > intra-vzdálenost.“* [18]

Díky identifikovatelnosti je možné s vysokou pravděpodobností možné od sebe odlišit jednotlivá zařízení stejného typu FNF. Identifikovatelnost je závislá na hodnotách intra- a inter-vzdáleností, respektive poměru mezi nimi. Rozložení vzdálenostních metrik je rozhodujícím faktorem v hodnocení možností identifikovatelnosti, tudíž ta sama závisí na přesném shromažďování kontrolních dat [10].

1.3.4 Fyzická neklonovatelnost

Fyzická neklonovatelnost je naprostým základem konceptu FNF, jak již z názvu vyplývá – fyzicky *neklonovatelná* funkce. Předpokládáme-li možnost, že by byl útočníka schopen kontrolovat podmínky vzniku, je přesto vyžadováno, aby nebyl schopen tento proces napodobit, tedy vyrobit dvě identická zařízení FNF. Dle Maese lze za identická zařízení lze považovat taková, u kterých je pozorováno stejné chování neboli obsahují stejnou dvojici párů výzva – odpověď [18]. V opačném případě by tím byla narušena jedinečnost FNF.

Definice fyzické neklonovatelnosti podle Maese zní následovně: *„FNF vykazuje fyzickou neklonovatelnost, jestliže je vyhodnotitelná a jestliže je obtížné ovlivnit její vznik takovým způsobem, aby bylo možno vytvořit dvě různé instance FNF, pro které by platilo,*

že je vysoká pravděpodobnost, že vzdálenost mezi jednotlivými instancemi FNF je menší než inter-vzdálenost.“ [18]

Fyzická neklonovatelnost také vyjadřuje, že je FNF odolné i vůči zásahům ze strany výrobce. Ačkoliv výrobce může kontrolovat průběh a podmínky během výroby, je pro něj přesné napodobení FNF instance stejně obtížné jako pro případného útočníka. Maes mluví o této skutečnosti, jako o *„odolnosti vůči výrobci“* [17].

1.3.5 Nepředvídatelnost

Nepředvídatelnost mezi odpověďmi slouží, jako dodatečné kritérium pro zabezpečení vzniku dvojic výzva – odpověď. Definice nepředvídatelnosti je podobná té jež je věnována fyzické neklonovatelnosti: *FNF vykazuje nepředvídatelnost, jestliže je vyhodnotitelná a jestliže je pravděpodobnost, že vzdálenost mezi již existující instancí FNF a vzdáleností predikované instance FNF je menší než inter-vzdálenost.“* [18]

Předpověď náhodné instance FNF lze rozdělit do dvou kroků – na část učící a tzv. vyzývací. Během inicializační fáze je předpokládáno, že je útočník schopen zachytit určité množství dvojic výzva – odpověď. Proto je mu buďto náhodně přiděleno určité množství výzev (tento postup má za úkol simulovat FNF s tzv. slabou nepředvídatelností) nebo je vzorek párů selektivně vybrán (takovýto případ reprezentuje tzv. silnou nepředvídatelnost) [10].

V následujícím kroku určeném pro vyzývání je učenému algoritmu předložena neznámá výzva. Algoritmus však na základě znalosti předchozích párů dokáže na danou výzvu odpovědět. Jestliže je vzdálenost predikované odpovědi menší než práh akceptovatelnosti odpovědi, tato skutečnost je vyjádřena inter-vzdáleností, tak je algoritmus schopen úspěšně napodobit odpověď FNF.

1.3.6 Matematická a skutečná neklonovatelnost

Na rozdíl od nepředvídatelnosti, která zvažuje pouze možnost, že útočník odchytí jistý omezený počet párů výzva – odpověď, tak matematická neklonovatelnost pracuje s hrozbou neomezeného přístupu. To znamená, že útočník je schopen jednak zachytit neomezené množství párů a zároveň má vlastní přístup k zařízení obsahující FNF. V takovém případě je možné, že je útočník schopen odpozorovat chování FNF instance nad rámec fungování komunikace výzva – odpověď. [18]

„FNF vykazuje matematickou neklonovatelnost, jestliže je nepředvídatelná, i když není limitován přístup k FNF instanci během učící fáze.“ [18] Z definice matematické neklonovatelnost je zřejmé, že je odvozena od nepředvídatelností.

Maes ve svém díle také poukazuje na nutnost velkého množství výzev, jelikož by jinak mohlo dojít k získání příliš velkého až veškerého množství párů výzev-odpověď. V takovém případě by útočník nemusel odpovědi ani hádat, pouze by je dosazoval z

databáze. Stejně tak je matematická neklonovatelnost podmiňována nemožností natrénovat algoritmus malým počtem výzev [18].

Skutečná neklonovatelnost instance FNF byla dříve v materiálech rozdělena na matematickou a fyzickou. Tedy na matematickou neklonovatelnost reakce FNF na výzvu a neklonovatelnost fyzickou, která reprezentovala nemožnost vytvoření identického zařízení. Aby bylo FNF skutečně neklonovatelné, musí splňovat současně obé podmínky. *„FNF instance vykazuje skutečnou neklonovatelnost, jestliže je zároveň fyzicky i matematicky nepředvídatelná.“* [18]

1.3.7 Jednosměrnost

Pappuem [19] označil jednosměrnost neboli složitost dohledání inverze k funkci za zásadní vlastnost konceptu FNF. Maes jednosměrnost definuje následovně: *„FNF vykazuje jednosměrnost, jestliže je vyhodnotitelná a jestliže k náhodné instanci FNF neexistuje inverzní algoritmus schopný nalézt výzvu, jejíž odpověď by byla podobna odpovědi náhodné instance FNF.“* [18].

1.3.8 Detekovatelnost manipulace

Manipulace neboli neoprávněný zásah do celistvosti systému, jež má za cíl trvale změnit jeho chování [18]. Manipulací je také myšlena eventualita, kdy se útočník pokouší o obejití zařízení FNF [14].

Vzhledem ke skutečnosti, že jednou ze zásadních vlastností fyzicky neklonovatelných funkcí vnitřní náhodnost, je jakýkoliv fyzický zásah do integrity instance provázen změnami, které se projeví na vztahu dvojice výzva – odpověď [18].

„FNF vykazuje detekovatelnost manipulace, jestliže je vyhodnotitelná a jestliže jakákoliv fyzický zásah má patrný efekt na chování FNF.“ [18]. Tedy manipulace s FNF zařízením má za výsledek neslučitelnost veškerých párů výzva – odpověď.

Z detekovatelnosti manipulace plyne nejen znalost o útoku na FNF instanci, ale zároveň i zamítnutí přístupu útočníkovi. Ve chvíli provedení fyzického útoku na FNF instanci dojde ke změně zdroje náhodnosti, tím pádem ztrácí FNF funkčnost a nemůže útočníka autorizovat [10].

1.4 Výhody a nevýhody fyzicky neklonovatelných funkcí

Hlavními výhody FNF je převážně zmírnění finanční náročnosti a zároveň navýšení úrovně zabezpečení oproti klasickým kryptosystémům. Jelikož se však jedná o pionýra na poli kybernetické bezpečnosti, je zapotřebí podotknout, že výše uvedené přednosti jsou pouze zatím předpokládané. Podobně tomu je i u níže uvedených nevýhod.

1.4.1 Výhody FNF

Bavíme-li se o primárních výhodách fyzicky neklonovatelných systémů, máme nejčastěji na mysli jejich cenovou nenáročnost a zvýšenou bezpečnost oproti klasickým kryptosystémům.

Zvýšenou bezpečností je u FNF míněn ten fakt, že kryptosystémy vytvořené jejich pomocí jsou odolné vůči reverznímu inženýrství. Také FNF neukládají citlivá data, jako např. šifrovací klíče, do napěťově nezávislé (neboli nevolatilní) paměti.

Ovšem, co se finanční nenáročnosti týká, nelze zaujmout jednotné stanovisko, jelikož již pořizovací cena jednotlivých zařízení na bázi fyzicky neklonovatelných funkcí není identická. Rovněž můžeme hovořit o různorodosti následných nákladů spojených s manipulací s FNF, jako jsou: výpočetní náročnost, spotřeba energie, nároky na prostor aj. Obecně vzato lze říci, že fyzicky neklonovatelné funkce s minimálními nároky mohou představovat alternativu pro bezpečnostní řešení na nižších úrovních ochrany.

1.4.2 Nevýhody FNF

Ačkoliv je nepředvídatelnost odpovědi FNF (způsobena vnitřním šumem zařízení) považována za jednu z nejdůležitějších vlastností, její přílišná míra je naopak velmi nevhodná a pokládáme ji za nevýhodu.

Odpovědi obsahující takové neúměrné množství šumu (jinak také zašumělé) jsou zejména nevhodné pro přímé generování šifrovacích klíčů [4]. Zašumění odpovědí je možné eliminovat implementací protichybových kódů, čímž se ovšem navýší náklady potřebné na aplikaci zařízení.

Ačkoli jsou FNF imunní vůči reverznímu inženýrství, bylo již zaznamenáno určité množství úspěšně provedených útoků na několik typů FNF (např. Arbitr FNF, SRAM FNF aj. [20]). Jednalo se o tzv. modelující útoky, využívající učících algoritmů, které jsou po odsimulování dostatečného množství formování párů výzva – odpověď schopny předpovídat chování instance FNF.

Další nevýhodou FNF zařízení je náchylnost na útoky postranními kanály [18]. Tento druh útoku představuje pro fyzicky neklonovatelné funkce skutečnou a relevantní hrozbu, jelikož napadá jejich samotnou podstatu. Útok postranními kanály nezasahuje do vlastní struktury objektu, čímž obcházejí obranný mechanismus FNF, a ani nezpůsobí změnu chování instance FNF.

2 Druhy fyzicky neklonovatelných funkcí

Obsahem této kapitoly je soubor všech dosud známých instancí FNF, které lze v literatuře dohledat. Sborník obsahuje některé konstrukce, které ve svém prvopočátku nebyly za FNF považovány, s ohledem na jejich vlastnosti můžeme však tvrdit, že do této podskupiny rovněž spadají.

Rozsáhlý seznam FNF lze rozdělit do několika kategorií, a to převážně v závislosti na jejich konstrukčních a provozních principech [17]. Bohužel ne všechny uvedené instance jsou zdokumentovány tak do hloubky, jako jiné. Tato skutečnost je způsobena převážně kvůli nedostatku dostupné literatury nebo proto, že některé konstrukce byly zmíněny pouze pro úplnost.

2.1 Neelektrické fyzicky neklonovatelné funkce

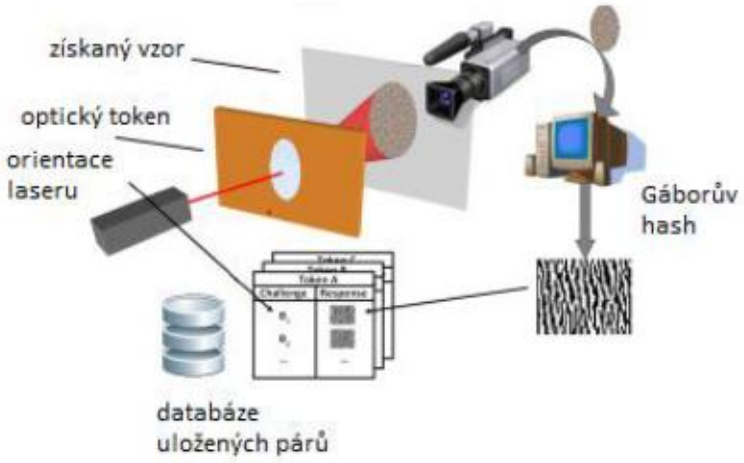
V této kapitole je uveřejněno několik konstrukcí a vlastnostmi blízkými těm FNF, které lze ze své podstaty řadit mezi neelektrické. Nicméně velmi často je v určitém okamžiku užito elektrických a digitálních technik ke zpracování a uložení FNF instancí efektivním způsobem.

2.1.1 Optické FNF

Raná verze optických fyzicky neklonovatelných funkcí byla představena již v roce 1992 [23], tedy několik let před zavedením pojmu FNF, pod termínem „*Reective Particle Tag“*. Tato varianta byla použita k identifikaci strategických, převážně nukleárních zbraní ve smlouvách o kontrole zbraní. Na toto pojednání později nepřímo navazuje Pappu, který na jejich bázi v roce 2001 [19] definoval základní koncept fyzicky neklonovatelných funkcí.

Základním prvkem designu optických FNF je optický token, který obsahuje optickou mikrostrukturu vytvořenou smícháním mikroskopické refrakční skleněné koule zasazené do průhledné epoxidové desky. Token je ozařován helium-neonovým laserem, to vzniklá vlnoplocha se stává velmi nepravidelnou kvůli vícenásobnému rozptylu paprsku s refrakčními částicemi [19]. Vzniklý vzor je následně nasnímán CCD (*Charge-Coupled Device*) snímačem a digitálně zpracován. K tomu je využito tzv. Gaborova hashe, který přepracuje pozorovaný skvrnitý vzor jako postup extrakce prvků do podoby bitového řetězce. Ten reprezentuje hodnotu hashe[22]. Základní implementace a provoz optického PUF je graficky znázorněn na obrázku 2.1.

Podoba výsledné výstupní hodnoty (odpověď) je závislá jak na umístění tokenu, tak i na přesném nasměrování světelného zdroje. Proto musí budící výzva obsahovat i detailní informace o umístění laseru.



Obrázek 2.1 Princip optických FNF, převzato z [10].

2.1.2 Papírové FNF

Zásady papírových fyzicky neklonovatelných funkcí byly představeny již v roce 1983 [1]. Patří tedy společně s optickými FNF mezi jedny z nejstarších představitelů této skupiny. Před uspořádaným zavedením konceptu FNF a byla tato forma považována převážně za strategii proti padělání bankovek [1].

Princip činnosti papírových FNF, tak jak ho dnes známe, vychází z řady návrhů z literatury, které v zásadě spočívají ve skenování jedinečné struktury běžného nebo pro potřeby snímání speciálně upraveného papíru [17]. Skenování je prováděno laserovým paprskem, získané nerovnoměrnosti vlákna vytvářejí unikátní vzor [12]. Roku 1993 byla metoda výroby vzorového papíru zdokonalena přidáním ultrafialových vláken [3]. Tato změna vedla k ulehčení snímacího procesu, jelikož již nebylo potřeba používat ke získávání jedinečné šablony laser, ale postačil obyčejný skener [3]. Ve téže práci byl také představen návrh dalšího typu papírového FNF. Na základě obsahu dat daného listu je vygenerován digitální podpis dat, který je obohacen o nahodilosti vlákna a následně je tento klíč na list vytištěn [10].

2.1.3 CD FNF

Maes ve své disertační práci [18] pojednává mimo jiné o tomto druhu FNF a to, že měřené délky ploch a vrypů na běžných kompaktních discích obsahují náhodnou odchylku od jejich zamýšlených délek kvůli pravděpodobnostním změnám během výrobního procesu. Tato odchylka je dokonce dostatečně velká, aby ji bylo možné sledovat pomocí signálu fotodetektoru v běžném CD přehrávači.

2.1.4 RF – DNA FNF

Návrh vysokofrekvenčního typu fyzicky neklonovatelných funkcí neboli RF-DNA FNF (*Radio-Frequency DNA PUF*) byl představen již v roce 2005[5].

Ke konstrukci RF-DNA FNF je užito podobně jako u optických FNF tokenu, který je v tomto případě tvořen poddajným křemíkovým materiálem (nejčastěji o rozměrech 25–50–3 mm), do kterého jsou náhodně umístěny měděné drátky obalené silikonovým tmelem. Zdroj náhodnosti RF-DNA FNF představuje rozptyl elektromagnetických vln v kmitočtovém spektru na různých vlnových délkách, zejména v pásmu 5–6 GHz. Tyto odchylky jsou způsobeny vnitřními vlastnostmi drátků, jako např. vodivostí [18].

Náhodné rozptylové efekty jsou měřeny prototypovým skenerem, který se skládá z matice RF antén. Entropie jediného tokenu se odhaduje na 50000 bitů [18].

2.1.5 Magnetické FNF

Podobně, jako v případě optických, či papírových, tak i návrh magnetických fyzicky neklonovatelných funkcí byl představen počátkem devadesátých let. Konkrétně v roce 1994 [12]. Jejich využití je převážně zaměřeno na zabezpečení platebních karet [4].

Princip magnetických FNF tkví ve využívání jedinečného vzoru částic v magnetickém médiu. Tento vzor je nabit během výrobního procesu, kdy je na zařízení nanesena magnetická vrstva složená z částic feritu barnatého ($BaFe_{12}O_{19}$), jehož částice mají rozdílnou velikost, a dokonce i tvar. To vše je navíc posíleno faktem, že jsou tyto částice na zařízení nanášeny náhodně. To vše vede k tomu, že je velmi nepravděpodobné rozložení částic na dvou zařízeních duplikovat [12]. Rozložení částic nelze kontrolovat a je tedy vhodným zdrojem náhodnosti fyzicky neklonovatelných funkcí [17].

2.1.6 Akustické FNF

Zdrojem náhodnosti akustických FNF jsou akustické zpožďovací linky. Samotný princip akustických fyzicky neklonovatelných funkcí spočívá v měření odezvy na akustickou vlnu. Vstupní elektrický signál je převeden na mechanické vibrace, které se šíří prostorem v podobě akustické vlny, která je následně tříštěna o náhodně distribuované nesourodosti [24]. Následně jsou odrazy vln měřeny zpožďovací linkou, která transformuje vibrace zpět na elektrický signál. Odrazy jednotlivých FNF instancí jsou unikátní.

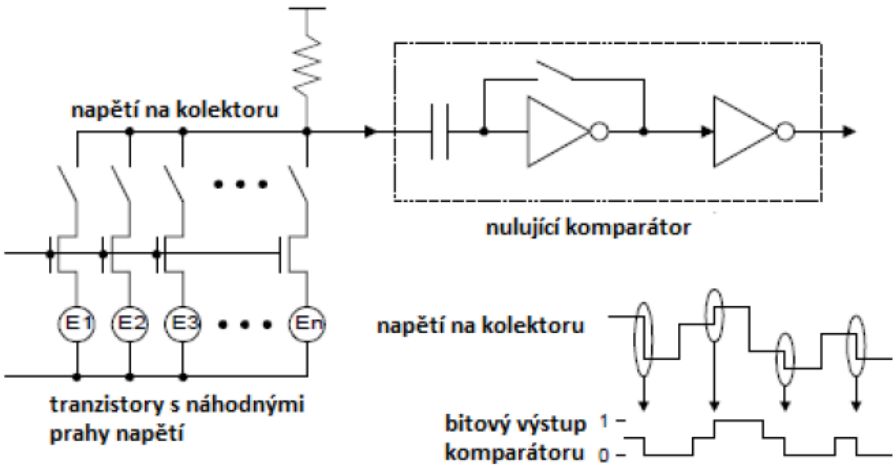
2.2 Analogové fyzicky neklonovatelné funkce

Tato kapitola pojednává o několika typech konstrukcí FNF, jejichž základní koncept spočívá v analogovém měření elektrické nebo elektronické veličiny. To na rozdíl od konstrukcí představených v kapitole. 2.1, kde měřená veličina byla ze své podstaty neelektronická, a návrhů v kapitolách. 2.3 a 2.4, kde jsou měření prováděna digitálně, zde se měření neobejde bez nutnosti použití analogových přístrojů.

2.2.1 FNF napěťového prahu

Metoda identifikace založená na náhodnostech ve výrobě neboli ICID (*Integrated Circuit IDentification*) byla prezentována již v roce 1999 [16], samozřejmě v této době pojem fyzicky neklonovatelné funkce nebyl stále znám. Proto ICID klasifikován jako FNF až zpětně [2].

Náhodnost je u FNF napěťového prahu zajištěna odchylkami během výrobního procesu, a to zejména rozmístění nečistot v kanálech tranzistorů [16].



Obrázek 2.2 Nákres principu FNF napěťového prahu. Převzato upraveno z [10].

K vlastní realizaci instance FNF jsou využity, z hlediska výrobce, identické tranzistory. Vlivem náhodností při výrobě nejsou napěťové prahy jednotlivých tranzistorů stejné, tím pádem se liší i procházejícím proudem na kolektoru. Napětí na kolektoru je měřeno a porovnáno automaticky nulujícím komparátorem. Následně je výstup překonvertován na bitové posloupnosti [10].

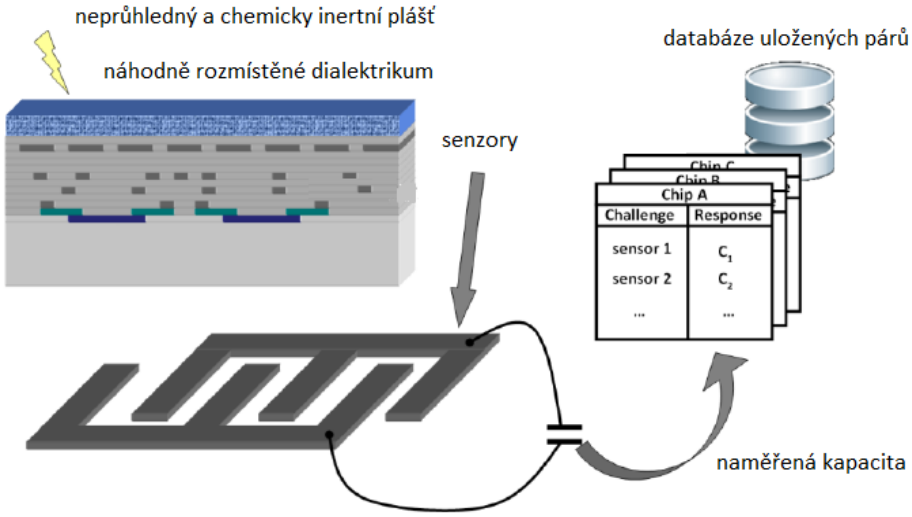
2.2.2 Power Distribution FNF

Koncept FNF založený na kolísání impedance [11] nebo na poklesu napětí na čipech představil Helinski v roce 2009. Zdroje náhodností jsou v obou případech nepřesnostmi vzniklé při výrobě.

Nevýhodou tohoto typu fyzicky neklonovatelných funkcí je nutnost měření externími přístroji a vysoká náchylnost na stabilní prostředí nutné pro reprodukovatelnost párů výzva – odpověď [10].

2.2.3 Plášťové FNF

Plášťové FNF vznikají aplikací ochranné vrstvy na integrovaný obvod. Nevyužívá se zde tedy náhodnosti vzniklé při výrobě, ale cíleně vytvořené. Ochranná vrstva obsahuje dielektrické částice o náhodné velikosti a rozmístění. Právě náhodnost umístění a velikosti zapříčiňuje náhodný charakter potřebný k realizaci FNF. Za výzvu systému lze tedy považovat měření kapacity FNF instance.



Obrázek 2.3 Základní operace plášťového FNF. Převzato, upraveno z [17]

Výstupem plášťového FNF je kapacita dielektrika ochranné vrstvy. Měřicí senzory jsou umístěny pod ochrannou vrstvou integrovaného obvodu ve tvaru napodobujícím hřeben v jedné řadě. Proces získávání hodnot je znázorněn na obr. 2.3.

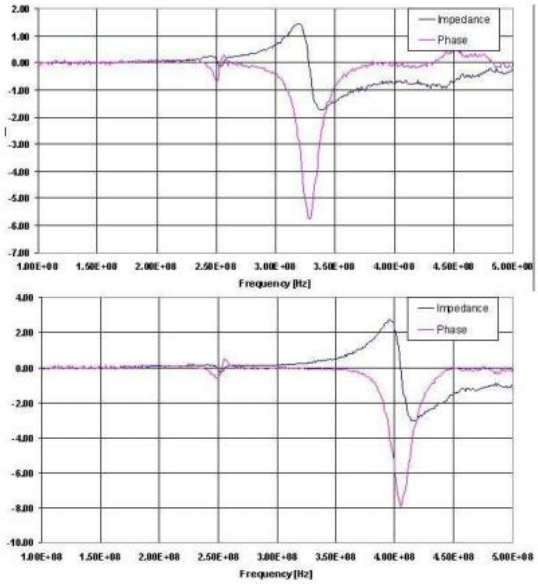
Výhodou plášťových FNF je neprůhledný plášť a jeho odolnost vůči vnějším, převážně chemickým a mechanickým vlivům [4]. Tento fakt tak komplikuje případné pokusy o fyzické napadení zařízení. Dojde-li k poškození pláště, bude to mít za následek nezvratnou změnu kapacity, a tedy i k zásahu do fungování FNF. Tento typ FNF je tedy schopen detekovat neoprávněnou manipulaci s produktem.

V [10] je zmíněna skutečnost, že ačkoliv není implementace plášťového FNF součástí výrobního procesu, ale je zapotřebí dodatečné akce, nejedná se o významné prodražení výrobku. Zároveň není nijak ovlivněna ani provozní cena zařízení, a ani nevznikají žádné zvýšené nároky na údržbu.

2.2.4 LC FNF

Fyzicky neklonovatelné funkce LC jsou odvozeny z principu plášťových FNF (měření kapacity), které byly představeny v roce 2009 [9]. V tomto případě je fyzicky neklonovatelná funkce realizována oscilačním obvodem, odtud název LC FNF a zdrojem náhodnosti jsou výrobní odchylky cívek a kondenzátorů.

Princip LC FNF je založen na využívání oscilačního obvodu, kde je obvod tvořen cívkou L a kondenzátorem C. V okamžiku, kdy je oscilační obvod vystaven působení radiofrekvenčního pole, absorbuje množství energie vytvořené frekvencí a vlastnostmi obvodu, které vyplývají z charakteristik cívek a kondenzátorů, ty jsou díky výrobním nahodilostem unikátní [9][17]. Jedinečnost jednotlivých obvodů lze pozorovat na průběhu rezonanční frekvence, ta je znázorněna na obrázku 2.4.



Obrázek 2.4 Rezonanční odezvy dvou různých LC FNF. Převzato z [9].

Primární výhoda těchto FNF se skrývá v odolnosti vůči teplotním změnám, jelikož je změna výstupních rezonančních křivek nepatrná (pozorování provedeno v teplotním rozmezí 25°C – 75°C) [9].

2.3 Fyzicky neklonovatelné funkce založené na zpoždění

V předchozích podkapitolách bylo představeno několik z celé řady zástupců, jejich podstata vychází z analogového měření náhodné fyzikální substance. Ta je později vyčíslena a lze ji použít jako unikátní identifikátor.

Tato podkapitola je však věnována tzv. vnitřním (intrinsickým) FNF zařízením. Tedy FNF, u kterých je náhodná substance prezentována vnitřní nestabilitou zařízení. Abychom mohli nazývat FNF zařízení vnitřním, musí splňovat dvě zásadní kritéria:

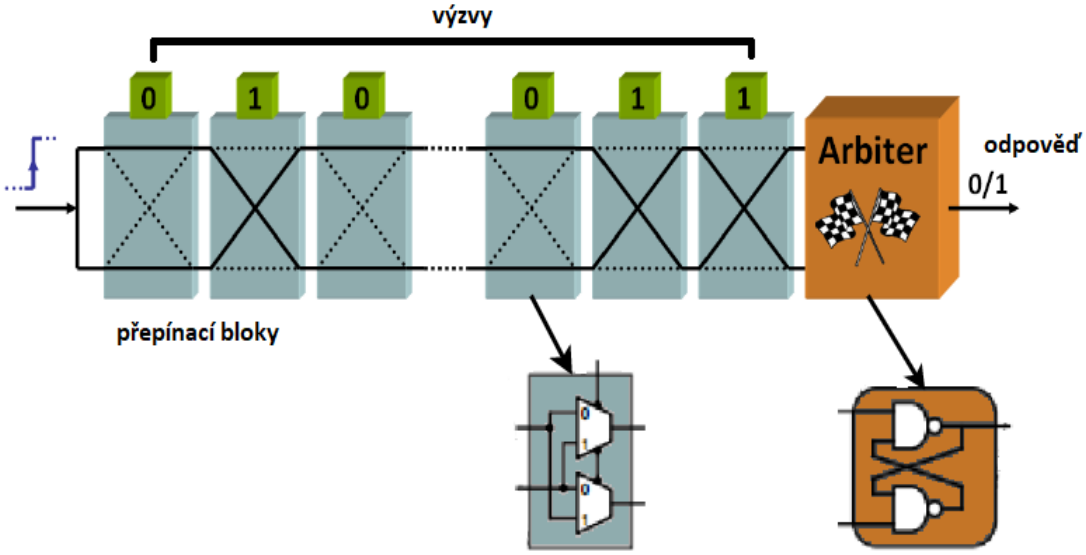
1) FNF, včetně měřicího zařízení, by mělo být plně integrováno do jediného zařízení.
2) Kompletní konstrukce FNF by měla sestávat ze součástí, které jsou přirozené ke konstrukci zařízení FNF obsahující.

2.3.1 Arbitr FNF

Arbitr FNF je jedním z představitelů FNF založených na časovém zpoždění. Původ náhodnosti arbitru FNF se zakládá na rozdílnosti zpoždění obvodů. Podmínkou je, aby obvody byly identické, tudíž takřka se stejným zpožděním [17]. V takovém okamžiku jsou vytvořeny potřebné (nepředvídatelné) podmínky pro určení obvodu s menším zpožděním, tím pádem je nepředvídatelný i výstupní bit.

Páry výzva – odpověď se v tomto případě utvářejí prostřednictvím „závodu“ (*race condition*) mezi dvěma symetrickými cestami signálu [17]. Tyto cesty vedou do cílového obvodu (tzv. *arbiter circuit*), kde určí, který obvod má menší zpoždění. Signál s menším zpožděním určuje povahu výstupního bitu.

V případě splnění výše uvedených podmínek (tj. identická konstrukce obvodů, skoro stejné zpoždění) uvádí Maes [17] dva možné scénáře chování návrhu FNF.



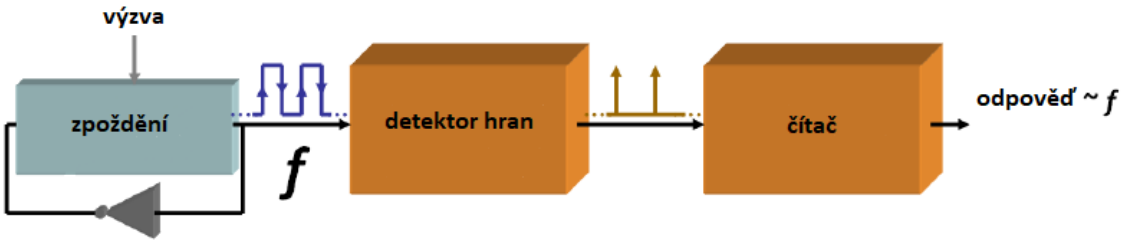
Obrázek 2.5 Schéma arbitru FNF. Převzato, upraveno z [17].

V prvním případě má dvojice cest markantní rozdíl ve zpoždění daný výrobními odlišnostmi. S ohledem na náhodnosti odchylek bude FNF, realizovaná tímto způsobem, individuální danému zařízení, a tedy i výstup bude danému zařízení specifický.

Při druhé variantě je zpoždění obou cest je téměř identické. Z čehož vyplývá, že bude závod nerozhodný. Arbitr v takovém případě dosáhne tzv. metastabilního stavu, kdy výstupní napětí nebude odpovídat ani jedné logické úrovni, nýbrž bude dosahovat hodnot mezi nimi [17]. Výstupní hodnota bude určena náhodně bez ohledu na „závod“. Odpověď je tedy náhodná, nicméně tato varianta není vhodná jako fyzicky neklonovatelná funkce, jelikož identická výzva nebude nutně generovat stejné odpovědi.

2.3.2 FNF kruhových oscilátorů

Další fyzikálně neklonovatelnou funkcí využívající koncept zpoždění jsou FNF kruhových oscilátorů. Tento typ byl poprvé představen Gassendem a kolektivem v roce 2002 [6]. Několik dalších autorů se tématu věnovalo a představili další variace FNF kruhových oscilátorů, jejichž konstrukce se lišila, ale princip zůstal stejný.



Obrázek 2.6 Měření zpoždění kruhového oscilátoru. Převzato a upraveno z [17].

FNF využívající kruhových oscilátorů jsou principiálně založeny na měření frekvence oscilujících obvodů. Zpoždění různých oscilátorů se liší v důsledku nekontrolovatelným vlivům během výroby digitálních součástek, které ovlivňují kruhové oscilátory, niž jsou součástí.

Kmitočet kruhového oscilátoru je ovlivněn použitými spoji a hradly. Typicky se konstrukce FNF skládá ze dvou základních částí: oscilujícího obvod a čítače frekvence [17], viz obr. 2.6. Čítač frekvence, složený z detektoru hran a samotného čítače, představuje obvod, který slouží k měření frekvence kruhového oscilátoru.

Na obrázku 2.6 můžeme vidět průběh získávání páru výzva – odpověď. Na vstup zpožďovacího obvodu je přiveden signál (výzva). Výstupem tohoto obvodu je jistý spojitý signál, který putuje do detektoru hran, kde se vyseparují vzestupné hrany signálu, které jsou následně zpracovány v čítači. V případě dostatečné komplexity obvodu je tato metoda vhodnou pro aplikaci FNF.

2.4 Paměťové fyzicky neklonovatelné funkce

Tato kapitola pojednává o druhu instancí fyzicky neklonovatelných funkcí, jenž je založen na usazování stavu primitiv digitální paměti. Digitální paměťová buňka je obvykle digitální obvod s více než jedním stabilním logickým stavem. Informace je ukládána právě pobytem v jednom ze zmíněných stabilních stavech, je-li však prvek uveden do stavu nestabilního, není zcela jasné, co nastane.

V jednom případě by mohla informace začít oscilovat mezi nestabilními stavy, v případě druhem muže dojít ke sloučení do jednoho ze stabilních logických stavů. V druhé variantě je pozorováno, že konkrétní buňky preferují určité stabilní stavy před ostatními. Tento fakt nelze logicky vysvětlit, ale je již známo, že to má, co dočinění

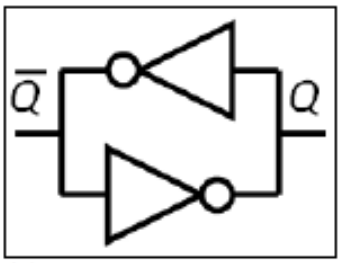
s vnitřním fyzickým nesouladem paměti. Díky tomu je stabilní stav usazování destabilizované paměťové buňky je dobrým kandidátem pro získávání odpovědí FNF.

2.4.1 SRAM FNF

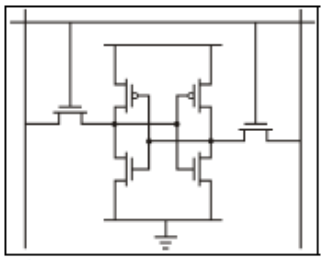
Statické paměti SRAM neboli *Static random-access memory* využívají bistabilních klopné obvody k uchovávání dat. SRAM se skládají z více paměťových buněk realizovaných pomocí křížově propojených invertorů. Každá tato buňka, respektive obvod, nabývá dvou stabilních hodnot – logická nula a logická 1. Jako FNF byly poprvé prezentovány roku 2009 [9]. Logický obvod paměti SRAM lze vytvořit, jak pomocí logických obvodů obr. 2.7, tak pomocí technologie MOSFET obr. 2.8 (zde je konkrétně užito standardu CMOS).

Funkčnost SRAM FNF je založen na skutečnosti, že jednotlivé paměťové buňky mají tendenci nabývat vždy identické hodnoty čili logickou 1 nebo 0, z čehož jednu z těchto hodnot buňka vždy preferuje. Zároveň však existují i buňky, které touto vlastností nedisponují [17].

Preference buněk paměti ohledně ustáleného stavu jsou nepředvídatelné. Také nemůže být určeno, zdali tyto buňky nebyly ovlivněny vnějšími vlivy. S ohledem na náhodnost charakteru a přirozené nezávislosti jsou tedy stabilní buňky SRAM vhodným prostředkem k realizaci fyzicky neklonovatelných funkcí [10].



Obrázek 2.7 Logický obvod buňky paměti SRAM. Převzato z [17].



Obrázek 2.8 Elektrický obvod buňky SRAM ve standardu technologie CMOS. Převzato z [17].

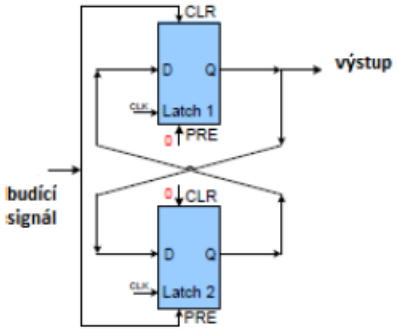
2.4.2 Butterfly FNF

Návrh Butterfly FNF [15] je alternativní konstrukcí, využívanou v případě, kdy není možno použít SRAM FNF z důvodu vyprazdňování paměti, např. v případě programovatelného hradlového pole FPGA (*Field Programmable Gate Array*). Zde nejde využít konceptu paměťových FNF, jelikož u běžných FPGA je při zapnutí paměť prázdná. Nemožnost využít nahodilých hodnot buněk po sepnutí je zároveň výhodné, jelikož instanci FNF můžeme kdykoliv vyvolat, čímž odpadá nutnost uložení odpovědi instance do paměti či účelové zapínání zařízení.

Butterfly FNF jsou svým chováním velice podobné SRAM FNF. Po vybuzení resetujícím signálem je integrovaný obvod přiveden do nestabilního stavu. Po ustálení získají jednotlivé buňky nahodilé hodnoty.

Jak je vidět z obrázku 2.9, Butterfly FNF je tvořeno dvojící nakříž propojených klopných obvodů. Budící signál (nastavený na hodnotu 1) vybudí vstupy klopných obvodů *preset* (PRE) a *clear* (CLR). Signál *clock* (CLK) následně převádí vstupní signál na výstupní. Tím je obvod přiveden do nestabilního stavu. Po uplynutí předem definovaného počtu taktů je budící signál vypnut (nastaven na hodnotu 0) a následně dochází k ustálení obvodu. Ustálený stav instance FNF je závislý na rozdílech ve zpoždění propojení jednotlivých klopných obvodů, které jsou dány výrobními nedokonalostmi a jsou tedy unikátní pro jednotlivá zařízení [14].

Důležitou podmínkou pro správnou funkci obvodu je přesné zpracování klopných obvodů. V případě přílišné nedokonalosti by náhodné odchylky byly příliš markantní pro aplikaci Butterfly FNF nepoužitelné [18].



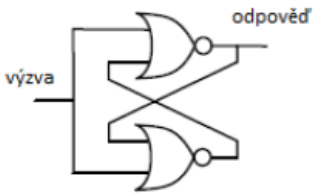
Obrázek 2.9 Schéma buňky Butterfly FNF. Převzato z [10].

2.4.3 FNF klopných obvodů

FNF využívající klopných obvodů, samotná konstrukce je vytvořena dvěma do kříže propojenými hradly NOR, byla představena již v roce 2007 [21].

Princip je založen na bistabilitě klopných obvodů. V klidovém stavu jsou buňky ustálené a v případě vybuzení je obvod ustálen na určité hodnotě. Tato hodnota závisí na vnitřním nesouladu hradel, který je vhodným zdrojem náhodnosti FNF [10].

Výzvu zde tvoří budící signál, který je přiveden na vstup. Odpověď tvoří logická hodnota. Její podoba je ovlivněna odchylkami při výrobě hradel, což ji dělá pro daná zařízení unikátní [17].



Obrázek 2.10 Jednoduché schéma FNF klopných obvodů.

Skutečnost, že zdroj náhodnosti FNF nespočívá v hodnotách po sepnutí je výhodou, jelikož může být hodnota FNF získána kdykoliv během aktivního fungování pouhým vybuzením obvodu [10].

2.4.4 Flip – Flop FNF

Princip chování Flip-Flop FNF je podobný FNF u klopných obvodů. Odlišností je využití klopných obvodů typu D. Podobně jako u FNF klopných obvodů je i na vstup Flip-Flop FNF přiveden signál reset, který uvede integrovaný obvod do neustáleného stavu. Po opětovném dosažení stability obvodu, mají jednotlivé klopné obvody typu D náhodně nabyté logické hodnoty [20].

Stejně, jako u fyzicky neklonovatelných funkcí klopných obvodů i zde platí, že budící signál může být kdykoliv opětovně přiveden na vstup obvodu, tudíž odpověď FNF instance může být opětovně vygenerována.

3 Komparativní analýza fyzicky neklonovatelných funkcí

V předchozí kapitole bylo představeno několik zástupců fyzicky neklonovatelných funkcí. S ohledem na pestrost konceptů FNF je téměř nemožné porovnávat jednotlivé typy na základě pouze jediného kritéria. Proto byla za účelem vzájemného porovnání typů FNF stanovena čtyři zásadní měřítka:

- Zdroj náhodnosti
- Způsob utváření párů výzva – odpověď
- Vlastní jednotlivých druhů FNF
- Obecné parametry

Tato čtyři kritéria pro vzájemnou komparaci různých druhů FNF stanovil ve své diplomové práci pan Hégr [10]. S ohledem na jejich výstižnost byla zvolena i pro níže uvedenou analýzu.

3.1 Klasifikace na základě zdroje náhodnosti

Náhodnost neboli také neklonovatelnost je jednou z nejdůležitějších a zřejmě nejcennější vlastností FNF. Právě díky tomuto atributu jsou FNF tak zajímavou komoditou v oblasti moderní kryptografie. V níže uvedené tabulce 3.1 jsou pro každý druh fyzicky neklonovatelné funkce vytyčeny tři důležité body, které pomáhají k jejich hlubšímu prozkoumání. Těmito body jsou:

- zdroj náhodnosti,
- její původ,
- zdali se jedná/nejedná o přirozené funkce.

V případě, jedná-li se o funkce přirozené bývá původ jejich nahodilosti ve většině případů způsoben odchylkou vzniklou při výrobě anebo fyzikálními vlastnostmi typickými pro dané druhy FNF. V opačném případě je nahodilost výsledkem invazního zásahu vůči zařízení ze strany člověka. Jedná se tak o cílené vytvoření zdroje fyzicky neklonovatelné funkce.

Zdroje náhodnosti:			
Neelektrické FNF:			
Druhy:	**Zdroj náhodnosti:**	**Původ náhodnosti:**	**Přirozená:**
optické FNF	náhodný vzor částic	vkládání drobných částiček	Ne
papírové FNF	náhodný vzor částic	vkládání drobných částiček	Ne
CD FNF	mechanická vzdálenost vrypů a plošek	výrobní odchylka	Ano
RF-RNA FNF	rozptyl elektromagnetických vln	dodaný vzor měděných drátků	Ne
magnetické FNF	náhodný vzor částic	dodaná magnetická vrstva	Ne
akustické FNF	náhodné nehomogenity	výrobní odchylka	Ano
Analogové FNF:			
Druhy:	**Zdroj náhodnosti:**	**Původ náhodnosti:**	**Přirozená:**
FNF napěťového prahu	nečistoty v kanálech tranzistorů	výrobní odchylka	Ano
Power Distribution FNF	kolísání impedance	výrobní odchylka	Ano
plášťové FNF	kapacita dielektrických částic	dodané dielektrické částice	Ne
LC FNF	odchylky cívek a kondenzátorů od nominálních hodnot	výrobní odchylka	Ano
FNF založené na zpoždění:			
Druhy:	**Zdroj náhodnosti:**	**Původ náhodnosti:**	**Přirozená:**
arbitr FNF	různé zpoždění prvků	výrobní odchylka	Ano
FNF kruhových oscilátorů	různé zpoždění prvků	výrobní odchylka	Ano
Paměťové FNF:			
Druhy:	**Zdroj náhodnosti:**	**Původ náhodnosti:**	**Přirozená:**
SRAM FNF	buňky preferují určitou logickou hodnotu	výrobní odchylka	Ano
Butterfly FNF	obsah paměti při spuštění	výrobní odchylka	Ano
CD FNF	vnitřní nesoulad hradel	výrobní odchylka	Ano
Flip-Flop FNF	vnitřní nesoulad hradel	výrobní odchylka	Ano

Tabulka 3.1 Zdroje náhodnosti

3.2 Klasifikace na základě utvoření páru výzva – odpověď

V tabulce 3.2 nalezneme přehled dříve vyjmenovaných typů FNF a k nim jejich specifikovaný způsob vytváření výzvy a podobu na ní závislé odpovědi. Výzvy jsou zpravidla tvořeny vstupními budícími signály, popřípadě jsou zdroje FNF vystaveny určitému druhu vnějšího vlivu, který odpověď vybudí.

Výzvy v podobě vstupního signálu mohou nabývat podob:

- elektrický signál,
- logický signál

Na druhou stranu mezi výzvy ve formě vnějšího vlivu může patřit:

- vystavení světelnému zdroji (např. laser, UV světlo apod.),
- vystavení RF poli,
- vystavení magnetickému poli,
- kolísání impedance,
- měření kapacity,
- dokonce i samotné spuštění zařízení.

Obdobně jako výzvy, tak i výstupní hodnoty, tedy odpovědi se mohou projevovat několika formami, jež lze opět rozdělit do dvou kategorií. A to na výsledky měření hodnot iniciovaných výzvou, kam patří:

- výsledná kapacita,
- změřená impedance,
- hodnota napěťového prahu,
- mechanická vzdálenost vrypů a plošek.

Druhou kategorií projevů výstupních hodnot jsou reakce FNF zařízení na vybuzení systému:

- unikátní vzor částic,
- logická hodnota,
- zpoždění,
- elektromagnetická vlna
- a jiné.

Získávání párů výzva – odpověď:		
Neelektrické FNF:		
Druhy:	**Výzva:**	**Odpověď:**
optické FNF	osvětlení zdrojem světla	unikátní vzor částic
papírové FNF	proměření laserovým paprsek	unikátní vzor částic
CD FNF	proměření laserovým paprsek	mechanická vzdálenost vrypů a plošek
RF-RNA FNF	vystavení RF poli	elektromagnetická vlna
magnetické FNF	vystavení magnetickému poli	hodnota magnetizace
akustické FNF	elektrický signál	odraz vlny
Analogové FNF:		
Druhy:	**Výzva:**	**Odpověď:**
FNF napěťového prahu	požadavek na zjištění napěťo-vého prahu	hodnota napěťového prahu
Power Distribution FNF	kolísání impedance	změřená impedance
plášťové FNF	měření kapacity	výsledná kapacita
LC FNF	vystavení RF poli	rezonanční frekvence
FNF založené na zpoždění:		
Druhy:	**Výzva:**	**Odpověď:**
arbitr FNF	elektrický signál	zpoždění
FNF kruhových oscilátorů	elektrický signál	zpoždění/frekvence
Paměťové FNF:		
Druhy:	**Výzva:**	**Odpověď:**
SRAM FNF	spuštění zařízení	logická hodnota
Butterfly FNF	logický signál	logická hodnota
CD FNF	logický signál	logická hodnota
Flip-Flop FNF	logický signál	logická hodnota

Tabulka 3.2 Získávání párů výzva – odpověď.

Po dosažení výstupní hodnoty se odpověď převede do číselné, nejčastěji bitové podoby, se kterou se nadále pracuje.

3.3 Klasifikace s ohledem na vlastnosti FNF

Jak již bylo zmíněno v kapitole 1.4, existence FNF je podmíněna šesticí vlastností, které musí být za každých podmínek splněny a pěti dalšími pravidly, jejichž přítomnost není pro zařízení FNF tak striktní, nicméně dále rozšiřují jejich definici (tyto vlastnosti jsou v níže uvedené tabulce odděleny od těch nezbytných dvojitou čarou).

Pro rychlé připomenutí. Vlastnosti, jež musí označení FNF splňovat, jsou:

- konstruovatelnost,
- vyhodnotitelnost,
- opakovatelnost,
- jedinečnost,
- identifikovatelnost,
- fyzické neklonovatelnost.

Tabulka 3.3 obsahuje přehledný výčet typů FNF, popsaných v kapitole 2 a jednotlivé vlastnosti, jimiž disponují. V tabulce se vedle odpovědí splňuje, či nesplňuje vyskytuje také parametr „není známo“. Tato odpověď znázorňuje fakt, že k takto označeným druhům není dostatečné množství dat, dle kterých by bylo možné zaujmout jednoznačné stanovisko.

Porovnáme-li tabulku 3.1 s tabulkou níže uvedenou, můžeme vypozorovat jistou spojitost mezi množstvím splněných vlastností a tím, jsou-li FNF přirozené, či nikoli. Kupříkladu u cíleně vytvořených FNF je možné vypozorovat podporu detekovatelnosti manipulace, kdežto u FNF, které jsou sami o sobě zdrojem nepředvídatelnosti to s jistotou tvrdit nemůžeme.

Vlastnosti FNF:											
Druhy FNF:	**Konstruovatelnost:**	**Vyhodnotitelnost:**	**Opakovatelnost:**	**Jedinečnost:**	**Identifikovatelnost:**	**Fyzická neklonovatelnost:**	**Nepředvídatelnost:**	**Matematická neklonovatelnost:**	**Skutečná neklonovatelnost:**	**Jedinečnost:**	**Detekovatelnost manipulace:**
Neelektrické FNF:											
optické FNF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
papírové FNF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CD FNF	✓	✓	✓	✓	✓	✓	-	-	-	-	-
RF-RNA FNF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
magnetické FNF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
akustické FNF	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓
Analogové FNF:											
FNF napěťového prahu	✓	✓	✓	✓	✓	✓	x	x	x	x	✓
Power Distribution FNF	✓	✓	✓	✓	✓	✓	x	x	x	-	X
plášťové FNF	✓	✓	✓	✓	✓	✓	✓	x	x	x	✓
LC FNF	✓	✓	✓	✓	✓	✓	x	x	x	x	✓
FNF založené na zpoždění:											
arbitr FNF	✓	✓	✓	✓	✓	✓	-	x	x	x	-
FNF kruhových oscilátorů	✓	✓	✓	✓	✓	✓	✓	x	x	-	-
Paměťové FNF:											
SRAM FNF	✓	✓	✓	✓	✓	✓	✓	x	x	x	-
Butterfly FNF	✓	✓	✓	✓	✓	✓	x	x	x	x	-
CD FNF	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Flip-Flop FNF	✓	✓	✓	✓	✓	✓	✓	x	x	x	-

Legenda: ✓ splňuje x nesplňuje - není známo

Tabulka 3.3 Přehled vlastností FNF.

3.4 Klasifikace FNF s ohledem na obecné parametry

Pod pojmem obecné parametry FNF je možné si představit kritéria netechnického charakteru, podle kterých by se mohl vývojář bezpečnostního zařízení, založeného na principu FNF, při svém výběru konkrétního typu řídit. Takovými externími parametry např. jsou: bezpečnost, náklady na realizaci, náročnost provozu, či výpočetní nároky. Samozřejmě je možné takových obecných parametrů nalézt více, ovšem tuto čtveřici lze považovat při volbě zařízení za nejdůležitější.

Pojem bezpečnost vyjadřuje skutečnost, jsou-li z dřívějších dob známy úspěšně provedené útoky na konkrétní druhy FNF zařízení. Je-li tomu tak, je to v tabulce 3.4 znázorněno poznámkou „potvrzeny útoky“. V případě, že zařízení útoku odolaly, jsou považovány za „bezpečné“ a za situace, kdy k vyřčení jednoznačného soudu, není dostatečné množství údajů, je tato skutečnost vyjádřena komentářem „není známo“.

Pod pojmem náklady na realizaci a náročnost provozu si lze představit finanční nároky nutné k pořízení zařízení FNF a úkonům nezbytným k zavedení výzvy, potažmo získání následné odpovědi [10]. Náklady na realizaci vyjadřují počáteční peněžní hodnotu, kterou je třeba uhradit pro samotné pořízení vybavení, případně opatření atributů zajišťujících náhodnost FNF (např. optický token, aplikace magnetické vrstvy aj.). Z toho vyplívá, že intrinsické, tedy přirozené druhy fyzicky neklonovatelných funkcí jsou ve výsledku dostupnější, jelikož v jejich případě stačí uhradit pouze pořizovací náklady.

Jak již bylo řečeno, náročnost provozu představuje finanční náklady a úkony nutné k zavedení výzvy i získání následné odpovědi, ovšem na rozdíl od nákladů na realizaci, jsou v této sekci prezentovány výdaje nutné k pořízení snímačů nutných k utvoření párů výzva – odpověď. Komentářem „minimální“ můžeme najít u druhů FNF, které nevyžadují žádné externí úkony a k procesu vytváření databáze dvojic výzva – odpověď není zapotřebí žádných speciálních snímačů.

Výpočetní nároky obsahují situace, při nichž by mohlo dojít (při vyhodnocování páru výzva – odpověď) k navýšení výkonu. Nejsou-li zapotřebí žádné speciální úkony, nároky na výkon stroje jsou minimální [10].

Obecné parametry FNF:				
Neeleektrické FNF:				
Druhy:	**Bezpečnost:**	**Náklady na**	**Náročnost provozu:**	**Výpočetní nároky:**
optické FNF	bezpečné	nutnost vytvoření	měření komplexní	digit. zpracování a
papírové FNF	bezpečné	papír obsahující UV	laserový snímač,	minimální
CD FNF	není známo	pořizovací	externí měření	minimální
RF-RNA FNF	bezpečné	aplikace měděných	speciální snímač	nedostatek dat
magnetické FNF	bezpečné	aplikace	externí měření	minimální
akustické FNF	není známo	pořizovací	nedostatek dat	převod signálu
Analogové FNF:				
Druhy:	**Bezpečnost:**	**Náklady na**	**Náročnost provozu:**	**Výpočetní nároky:**
FNF napěťového	není známo	pořizovací	běžné	minimální
Power Distribution	není známo	pořizovací	externí měření	minimální
plášťové FNF	bezpečné	nutná aplikace	externí měření	minimální
LC FNF	není známo	pořizovací	externí měření	nedostatek dat
FNF založené na zpoždění:				
Druhy:	**Bezpečnost:**	**Náklady na**	**Náročnost provozu:**	**Výpočetní nároky:**
arbitr FNF	potvrzeny útoky	pořizovací	běžné	minimální
FNF kruhových	potvrzeny útoky	pořizovací	běžné	minimální
Paměťové FNF:				
Druhy:	**Bezpečnost:**	**Náklady na**	**Náročnost provozu:**	**Výpočetní nároky:**
SRAM FNF	potvrzeny útoky	pořizovací	běžné	minimální
Butterfly FNF	potvrzeny útoky	pořizovací	běžné	minimální
FNF klopných	potvrzeny útoky	pořizovací	běžné	minimální
Flip-Flop FNF	potvrzeny útoky	pořizovací	běžné	minimální

Tabulka 3.4 Obecné parametry FNF.

Cílem táto kapitoly bylo klasifikovat jednotlivé druhy instancí FNF a ulehčit tak jejich výběr pro případnou budoucí realizaci. Ačkoliv se přehled nejdůležitějších vlastností pro skupinu FNF nachází v tabulce 3.3, nejvýznamnějším parametrem pro výběr vhodného typu FNF jsou obecné parametry, tedy obsah tabulky 3.4. S ohledem na potenciál fyzicky neklonovatelných funkcí v oboru IoT je kladen důraz na jejich výpočetní nároky. Ze stejného důvodu by také bylo vhodné, aby případný kandidát byl zástupcem intrinsických, tedy přirozených typů FNF. Vezmeme-li v potaz tyto dvě skutečnosti a protneme je se srovnání na základě vlastností FNF, vycházejí nám dva nejvhodnější kandidáti. A to FNF kruhových oscilátorů, jakožto zástupce fyzicky neklonovatelných funkcí založených na zpoždění a SRAM FNF reprezentující paměťová FNF.

4 Využití fyzicky neklonovatelných funkcí v kryptosystémech

Jak bylo již v úvodu řečeno fyzicky neklonovatelné funkce lze přirovnat k biometrickému otisku prstu určitých typů zařízení. Tato vlastnost se hodí v kombinaci s předpřipravenou databází výzev a k nim předpřipraveným vzorovým odpovědím k identifikaci, popřípadě autentizaci přístroje disponující nějakou formou FNF zařízení.

Obdobně, jako u identifikace a autentizace je využito jedinečnosti odpovědi, jednoho z pěti atributů definující fyzicky neklonovatelné funkce, je tato vlastnost základem pro další obor v rámci kryptosystémů a tím je generování klíčů. Ovšem na rozdíl od dvou předchozích případů, není při generování klíčů nezbytně nutné vytvářet databázi výzev a odpovědí.

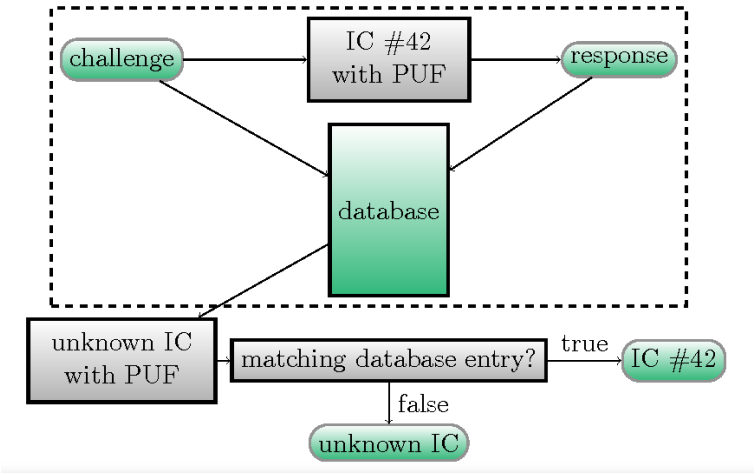
4.1 Autentizace

Na autentizace, jakožto na kryptografický obor jsou kladeny vysoké požadavky v podobě paměťové, výpočetní, ale i spotřební náročnosti. Tyto nároky se ovšem s aplikací fyzicky neklonovatelných funkcí snižují a v případě volby optimálního druhu FNF může rozdíl v nutnosti investice zdrojů nabývat i významných rozdílů.

Samotnému procesu autentizace musí předcházet inicializační neboli učící fáze. Tedy etapa, kdy se k jednotlivým zařízením utvářejí dvojice výzva – odpověď, kdy jsou na „syrový“ výstup FNF zařízení implementovány protichybové kódy, které jej přetvoří do podoby referenční odpovědi. Ta je následně společně s výzvou, která ji vyvolala uložena do databáze. Ta je ve většině případů uložena mimo autentizované zařízení, a to nejčastěji v centrálním zařízení celého systému. Popřípadě mimo celý systém, řídící jednotka k ní však přístup má.

Po ukončení inicializační fáze, se může přejít k samotné autentizaci, tedy k ověřovací fázi. Zde jsou výstupní hodnoty zařízení, vyvolané určitými výzvami, porovnávány se vzorovými odpověďmi získanými z databáze, které daným výzvám přísluší.

Samotný proces ověřování probíhá v několika krocích. Zařízení, jež žádá nebo je po něm žádána autentizace je zaslána výzva. Zařízení následně na základě přijaté výzvy vygeneruje odpověď. Ta je následně odeslána zpět k řídící jednotce, kde je nově vzniklá odpověď porovnávána s referenční odpovědí (odpovídající, výzvě, které byla na začátku poslána zařízení) z databáze. Jsou-li odpovědi vyhodnoceny jako shodné, je zařízení úspěšně autentizováno. V opačném případě je žádost považována za neplatnou a autentizace je zamítnuta.



Obrázek 4.1 Autentizační schéma. Převzato z [26].

Je předpokládáno, že komunikace mezi centrálním zařízením a zařízením s FNF probíhá v nedůvěryhodném prostředí, Je proto nutné, aby bylo pro ověřovací fázi připraveno velké množství párů, kdy je v ideálním případě každý pár využit pro ověření pouze jednou. Toto opatření slouží jako prevence před útokem typu MITM [26].

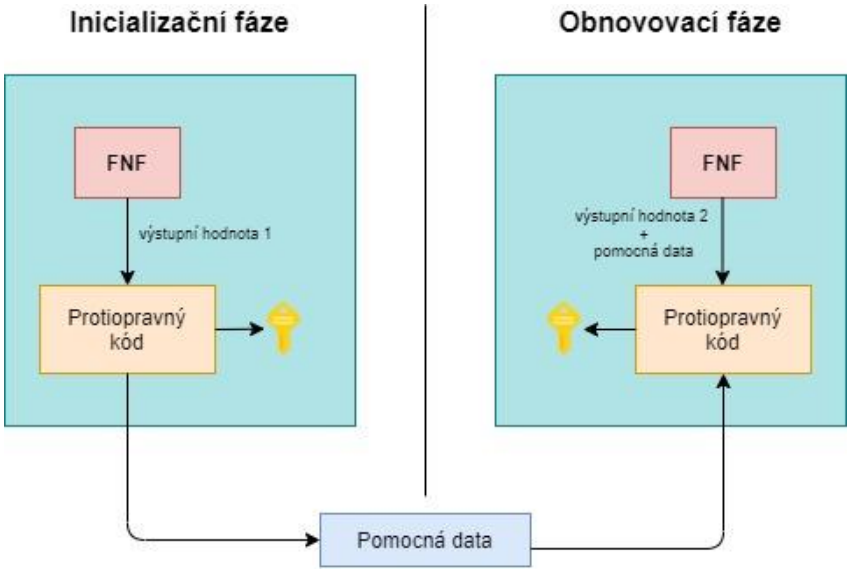
4.2 Generování šifrovacích klíčů

Šifrovací klíče jsou ve běžných kryptosystémech obvykle uloženy v nevolatilní paměti. Z toho důvodu vzniká potřeba tato uložiště zabezpečit proti různým druhům možných útoků. Taková bezpečnostní řešení bývají často velice výpočetně náročná a také finančně nákladná.

S možným zavedením fyzicky neklonovatelný funkcí do problematiky by mohly všechny dosavadní komplikace s generováním a ochranou šifrovacích klíčů odpadnout. Na rozdíl od standardních prostředků nabízí využití FNF levnější a v jistém ohledu také bezpečnější alternativu. Jelikož FNF umožňují generování výstupů v průběhu získávání dat, pozbývají tak nároky na provoz a zabezpečení stálého uložiště význam. Vhodnými kandidáty pro generování šifrovacích klíčů jsou například FNF klopných obvodů, či FNF kruhových oscilátorů.

Ovšem generování šifrovacích klíčů pomocí fyzicky neklonovatelných funkcí má i své nevýhody. Tou nejzásadnější je nativní chybovost odpovědí, tedy nestabilita výstupních signálů aparátů FNF. Aby bylo možné nově vytvořený klíč využít, musí mezi šifrovacími klíči panovat sto procentní bitová shoda. V případě, že by se opakovaný výstup lišil, byť v jediném bitu, mělo by to za výsledek nečitelnost dešifrovaných dat, tedy že by byla nově nabytá data z praktického hlediska naprosto bezcenná [27]. Tomu lze předejít aplikací protichybových kódů (1.2.4), které jsou uzpůsobené tak, aby co nejvíce snížili chybovost získaných hodnot. Užití samoopravných kódů sebou však nese negativum v podobě zvýšení výpočetní nároků na FNF zařízení.

Podobně, jako proces autentizace, tak i proces generování šifrovacích klíčů se skládá ze dvou fází. První fází je fáze inicializační. Avšak na rozdíl od autentizace se v tomto kroku nevytváří žádná obsáhlá databáze párů výzva – odpověď, nýbrž je generován pouze jeden jediný šifrovací klíč, ke kterému protichybový kód vytvoří pomocná data, která jsou v zařízení trvale uložena pro další užití. Pomocná data jsou obyčejně údaje veřejně známá, tedy přístupná. Je proto požadováno, aby nebylo možné získat šifrovací klíč reverzními metodami [14].



Obrázek 4.2 Schéma generování šifrovacích klíčů.

Druhou fází procesu je tzv. obnovovací fáze, kdy je šifrovací klíč reprodukován. Po opětovném vybuzení výstupu je na něj, z důvodu jeho případné neshody s šifrovacím klíčem vytvořeným během inicializačního kroku, implementován protichybový kód podpořený pomocnými daty. Výsledná podoba nově nabytého klíče je poté identická s šifrovacím klíčem vytvořeným během inicializační fáze.

4.3 Identifikace

Již v úvodu této práce byly fyzicky neklonovatelné funkce připodobněny biometrickému otisku prstů. Toto tvrzení není ve své podstatě realitě až tak vzdálená, jelikož FNF poskytují, stejně jako otisk prstu, o svém původci unikátní data, na základě, kterých je možné zařízení, ze kterého funkce pochází, identifikovat

S ohledem na technickou nenáročnost se v případě identifikace nejedná o žádnou krajně složitou činnost. Ačkoliv jsou výstupní hodnoty dvou FNF zařízení stejné kategorie, rozdílné z důvodu vnitřní nestability zařízení, obě reagují na stejný vstup. Právě tato interní nestálost způsobuje jedinečnost získaných odpovědí a je tedy oněmi unikátními daty, podle kterých je možné jednotlivá FNF zařízení stejného typu od sebe rozeznat (identifikovat).

Třebaže se i jednotlivé odpovědi jediného atributu FNF reagující na totožnou výzvu mohou od sebe nepatrně měnit, netvoří to v případě identifikace (na rozdíl od autentizace, či generování šifrovacích klíčů) žádný zásadní problém. Dokonce není ani nutné aplikovat na výstupní hodnoty protichybové kódy. Pro účely identifikace naprosto postačí, aby byla získaná odpověď dostatečně blízká referenční odpovědi daného zařízení získané během inicializační fáze, a zároveň dostatečně odlišná odpovědím jiných zařízení [27].

5 Návrh a tvorba softwarového systému s využívající fyzicky neklonovatelné funkce pro autentizaci

Následující kapitola se bude zabývat návrhem a následnou tvorbou softwarového autentizačního systému. To obnáší návrh SW řešení fyzicky neklonovatelné funkce, dále pak tvorbu jednoduché databáze párů výzva – odpověď a v neposlední řadě komunikaci mezi centrálním zařízením a zařízením disponujícím FNF.

Pro samotnou tvorbu aplikace byl zvolen programovací jazyk Python verze 3.9.4, a to pro svou všestrannost a současně jednoduchost. S ohledem na skutečnost, že je Python vyvíjen, jako open-source projekt, má za sebou velký zástup příznivců. Toto množství je velice dobře reprezentováno hojným počtem různých internetových blogů a fór.

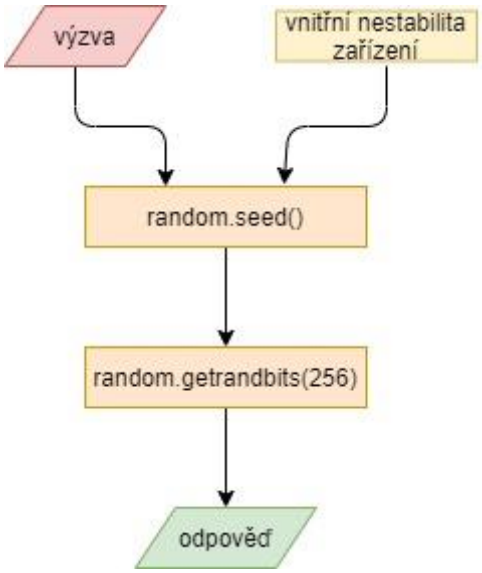
5.1 Návrh a tvorba funkce nahrazující fyzicky neklonovatelné funkce

Náhrada fyzicky neklonovatelné funkce patří samozřejmě mezi stěžejní části celé autentizační aplikace. Jelikož se jedná pouze o softwarovou modelaci FNF, výstup této instance bude vždy stejný. Na rozdíl od běžných výstupních hodnot FNF instancí, které mají nestabilní povahu. Z tohoto důvodu není nutné aplikovat na získané odpovědi žádnou formu protichybových kódů.

Pro samotné vytvoření nápodoby FNF bylo využito standartní knihovny programovacího jazyka Python, *random*, která slouží k implementaci generátorů pseudonáhodných čísel. Nejvyužívanějším takovým generátorem je Mersenne Twister. Z modulu *random* jsou pro tvorbu jedinečné odpovědi instance FNF použity dvě metody. Jsou jimi příkaz *seed()*, jež slouží pro inicializaci nadcházejícího generátoru náhodných čísel a metod *getrandbits()*, která vygeneruje náhodné číslo v rozmezí od pozice zadefinované metodou *seed()* až po hodnotu v ní vymezenou vymezenou. Jak název metody generující náhodné číslo napovídá, maximální velikost čísla, jež může generátor vyprodukovat je reprezentována počtem bitů. V našem případě se jedná o počet 256b. Tento proces je ve fyzické části této práce zaštítěn funkcí *facility()*.

Níže uvedený obrázek 5.1 reprezentuje schéma softwarové funkce sloužící, jako náhrada za reálné zařízení FNF. V horní části schématu můžeme vidět výzvu, vyvolanou z předpřipravené databáze, vstupujíc do bloku reprezentující metodu *seed()*, kde v kombinaci s vnitřní nestabilitou zařízení, ztělesněnou pevně definovanou hodnotou specifickou pro každé zařízení, tvoří inicializační bod od kterého bude nadcházející generátor začínat. Následný výstup generátoru reprezentuje výstupní hodnotu atributu

FNF, který může být buďto v rámci inicializační (učící) fáze uložen k příslušné výzvě do databáze nebo v průběhu ověřovací fáze užit k autentizaci zařízení.



Obrázek 5.1 Schéma funkce nahrazující FNF zařízení.

5.2 Návrh a tvorba databáze výzva – odpověď

Další nedílnou součástí autentizačního systému na základě fyzicky neklonovatelných funkcí je databáze výzev a k nim odpovídajících referenčních odpovědí pro jednotlivá zařízení. Tato databáze je přístupná pouze centrálnímu zařízení (výpočetně výkonnější zařízení, kterému se FNF zařízení autentizují), ať už v případě, že je jeho součástí anebo, že je databáze uložena na nějakém vzdáleném uložišti a centrální zařízení se k ní připojuje.

V našem případě byla zvolena druhá varianta umístění databáze, tedy vzdálené umístění referenční databáze pomocí MySQL serveru, ke kterému se pro správu a manipulaci s hodnotami uloženými v tabulce připojujeme. Pro správu MySQL databáze je nutné mít v zařízení, kde bude databáze uložena, tuto aplikaci nainstalovanou. Samotné připojení k databázovému serveru je řešeno pomocí modulu *mysql.connector*, který naneštěstí není standartní knihovnou programovacího jazyka Python, je proto nutné ji rovněž doinstalovat.

```
import mysql.connector

mydb = mysql.connector.connect(
    host="localhost",
    user="root",
    password="root",
    database="challenge_response_database"
)
```

Obrázek 5.2 Vzdálené připojení k databázi.

Po nainstalování modulu je možná se k databázovému serveru přihlásit pomocí příkazu *connect()*, ve kterém je nutné vyplnit údaje, které jsme volili při instalaci MySQL serveru. Jedná se o údaje o místě, kam se má program pro práci s databází připojit (v našem případě se jedná o adresu *localhost*), název a heslo uživatele. Po úspěšném připojení k serveru je možné vytvořit samotný databázový systém. Pro jeho vytvoření se použije SQL příkazu *„CREATE DATABASE“*, za který se vloží námi zvolený název databázového systému. Po vytvoření databáze je nutné i tuto položku do příkazu *connect()* přidat. Podoba příkazu pro připojení k databázi je znázorněna na obrázku 5.2.

Ve chvíli, kdy je spojení s databází připravené, je nezbytné vytvořit databázovou tabulku, kam budou ukládána data v podobně výzev a následných odpovědí jednotlivých FNF zařízení. K této tvorbě slouží příkaz „*CREATE TABLE“*, za který se, podobně, jako u příkazu pro vytvoření databáze, vkládá název tabulky a za ten do závorky názvy a vlastnosti jednotlivých sloupců.

V našem případě tabulka obsahuje čtyři sloupce. Jsou jimi:

- ID – automaticky plněný sloupec a nabývající hodnot 1 až n, slouží k výběru hodnoty challenge,
- výzva – do tohoto sloupce jsou vkládána data sloužící, jako vstupní hodnoty pro FNF zařízení. První hodnotu je zapotřebí vložit manuálně, další plnění je zajištěno automaticky během inicializační fáze (5.3),
- odpověď zařízení 1,
- odpověď zařízení 2,
- odpověď zařízení 3.

Sloupce odpověď zařízení 1-3 obsahují referenční hodnoty výstupů zařízení fyzicky neklonovatelných funkcí, které v našem případě nabývají formy dekadickýchch čísel o délce až 77 znaků. Tyto údaje jsou do tabulky přidány během inicializačního kroku. Tabulka 5.1 reprezentuje ukázku obsahu databáze výzva – odpověď po naplnění.

ID	Výzva	Odpověď zařízení 1	Odpověď zařízení 2	Odpověď zařízení 3
176	1009637	54280…11085	11188…73594	25801...27192
177	1009732	46403…21414	89579...49531	28366...70256
178	1009797	63842…98221	63892...44369	26766...22961
179	1009884	84886…19760	43183...31938	10384...50021
180	1009982	14851…29244	87000...23000	71090...45914
181	1010010	66756…45058	10891...90750	56269...61528
182	1010014	18818…73236	17121...58917	10662...70369
183	1010087	26997...63875	96496...27125	98469...30563
184	1010144	77018...90447	83465...40699	10690...93862
185	1010208	71916...57076	61049...75911	35638...59051

Tabulka 5.1 Obsah databáze výzva – odpověď.

5.3 Inicializační fáze systému

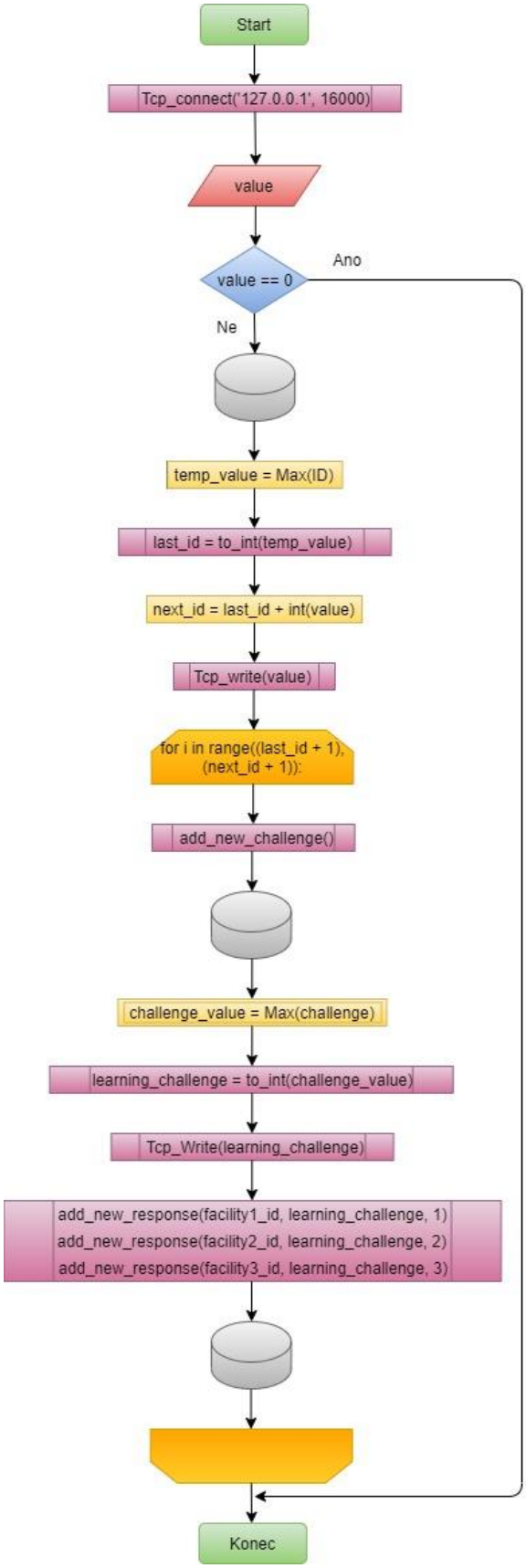
Inicializační krok je nepostradatelnou součástí jakéhokoli autentizačního systému. V tomto kroku se získávají referenční hodnoty, které později (při ověřovací fázi) slouží jako kontrolní vzor, se kterým je autentizační složka porovnávána. V našem případě se v této etapě plní databáze výzva – odpověď, a to jak vstupními hodnotami (výzvami), které jsou v závislosti na svém předchůdci vždy navýšeny o nepředvídatelnou hodnotu v rozmezí 1–99, tak i odpověďmi od FNF zařízení.

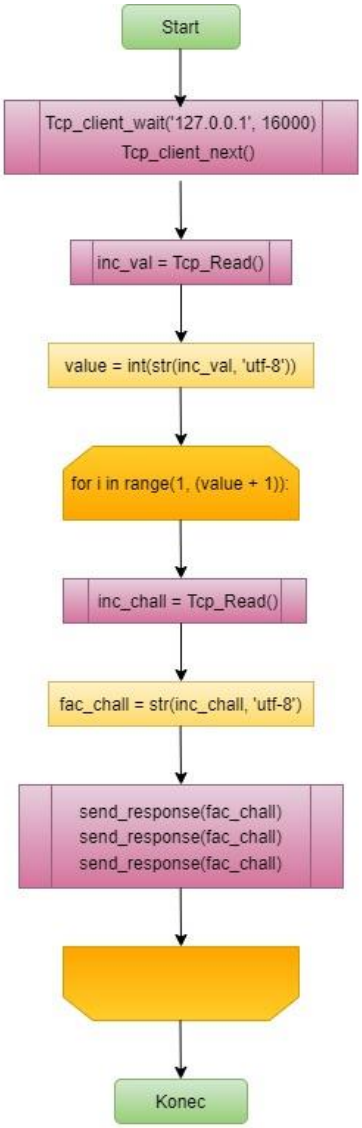
O tvorbu nové výzvy se stará funkce *add_new_challenge()*, jenž si na svém počátku zavolá z databáze polední uloženou hodnotu ve sloupci výzva, kterou si uloží do proměnné *int_value*. Tato proměnná je poté volána funkcí *db_value()*, která k údaji z databáze přičte náhodně vygenerované číslo z relace 1 – 99. Nově vzniklá hodnota je následně uložena zpět do databáze jako nová výzva.

Pro získání referenční odpovědi je nutné navázat spojení se zařízením disponujícím fyzicky neklonovatelnou funkcí. V našem případě je k tomu využito modulu *socket*, který obě zařízení propojí pomocí výchozího protokolu Transmission Control Protocol (TCP). Na rozdíl od knihovny *mysql.connector* je knihovna *socket* standartní součástí programovacího jazyka Python. Z toho důvodu ji není potřeba, obdobně jako v případě modulu random, doinstalovávat a postačí ji pouze na začátku aktivovat příkazem *import socket.*

Nabytí referenčního výstupu k nově vzniklé výzvě probíhá v rámci několika kroků probíhajících na obou stranách spojení. Nejprve je na straně centrálního zařízení (po navázání spojení se zařízením disponujícím FNF) vybrána z databáze nově vzniklá výzva, která je poslána pomocí funkce *Tcp_write()* FNF zařízení, tam je výzva přijata funkcí *Tcp_Read()*, po přenosu je dekódována a výsledná hodnota uložena do proměnné fac_chall. Posléze je ze strany centrálního zařízení posláno ID zařízení, jehož odpověď je žádána. Tento údaj je obdobně, jako výzva na straně zařízení přijat, dekódován a uložen do proměnné fac_id. Po přijetí všech potřebných údajů jsou tato data využita k vytvoření

jedinečné odpovědi pomocí funkce *facility()* (popis činnosti této funkce je popsán v kapitole 5.1). Nově vzniklá odpověď je následně odeslána centrálnímu zařízení, kde je přijata, dekódována a poté uložena k patřičné výzvě a zařízení do databáze výzva – odpověď. Tento proces se opakuje pro všechna FNF zařízení, která jsou součástí autentizačního systému. Z důvodu úspory místa jsou výše popsané procesy v níže uvedeném diagramu znázorněny jako volání funkce, a to *add_newresponse()* na straně centrálního zařízení (vlevo) a *send_response()* na straně zařízení FNF (vpravo).





Obrázek 5.3 Vývojový diagram iniciační fáze.

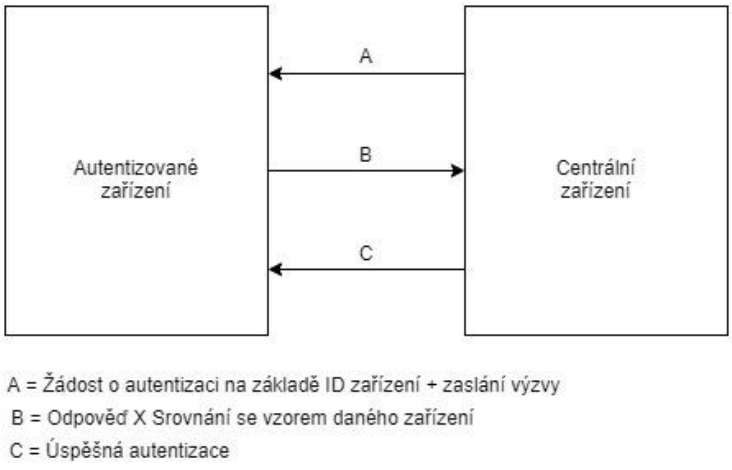
Jelikož jsou odpovědi během inicializační fáze posílána směrem k řídící jednotce nezabezpečeně, je nutné zajistit, aby komunikace mezi zařízeními po čas učící fáze probíhala po zabezpečeném kanále [4]. I tento fakt je zde zohledněn volbou jiného komunikačního portu než v případě ověřovací fáze.

5.4 Autentizace zařízení

Ověřovací krok je fází, při která se zúročí data nabytá při iniciační fázi. Autentizace zařízení disponující fyzicky neklonovatelnou funkcí se v našem případě dělí na ověření ze strany centrálního zařízení, kdy si centrální jednotka určí, po kterém FNF zařízení bude autentizace vyžádána a ověření ze strany FNF zařízení. V takovém případě se zařízení autentizuje řídící jednotce bez toho, aby k tomu bylo před tím z její strany vyzváno.

5.4.1 Autentizace ze strany centrálního zařízení

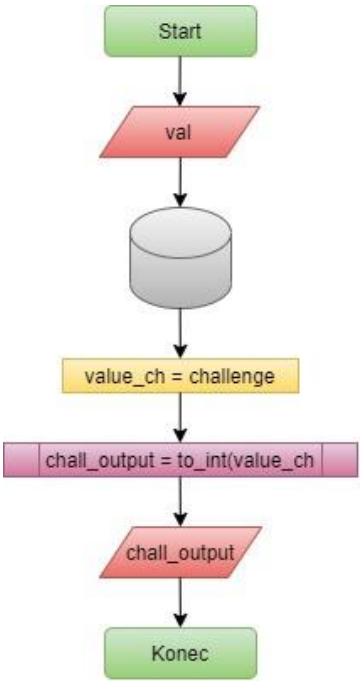
Samotná autentizace ze strany řídící jednotky probíhá v několika po sobě jdoucích krocích, kterým předchází navázání společné komunikace mezi centrálním a FNF zařízením.



Obrázek 5.4 Návrh autentizace ze strany centrálního zařízení.

Jako první je pomocí funkce *Tcp_Write()* FNF zařízení odesláno identifikační číslo stroje, po kterém je ověření vyžádáno. Následně je pomocí funkce *chall_selection()* (obr. 5.6) a náhodně vylosované hodnoty val v relaci 1 – n (kde n je id nejvyššího páru výzva – odpověď ze stejnojmenné databáze) nahodile vylosována výzva. I ta je posléze poslána FNF zařízení.

Zde jsou tyto dvě hodnoty, stejně jako při inicializační fázi, přijaty pomocí funkce *Tcp_Read(),* dekódovány a v závěru použity pro tvorbu odpovědi. Po vygenerování výstupu je tato hodnota odeslána zpět centrálnímu zařízení k ověření, tentokrát již v podobě hashe.



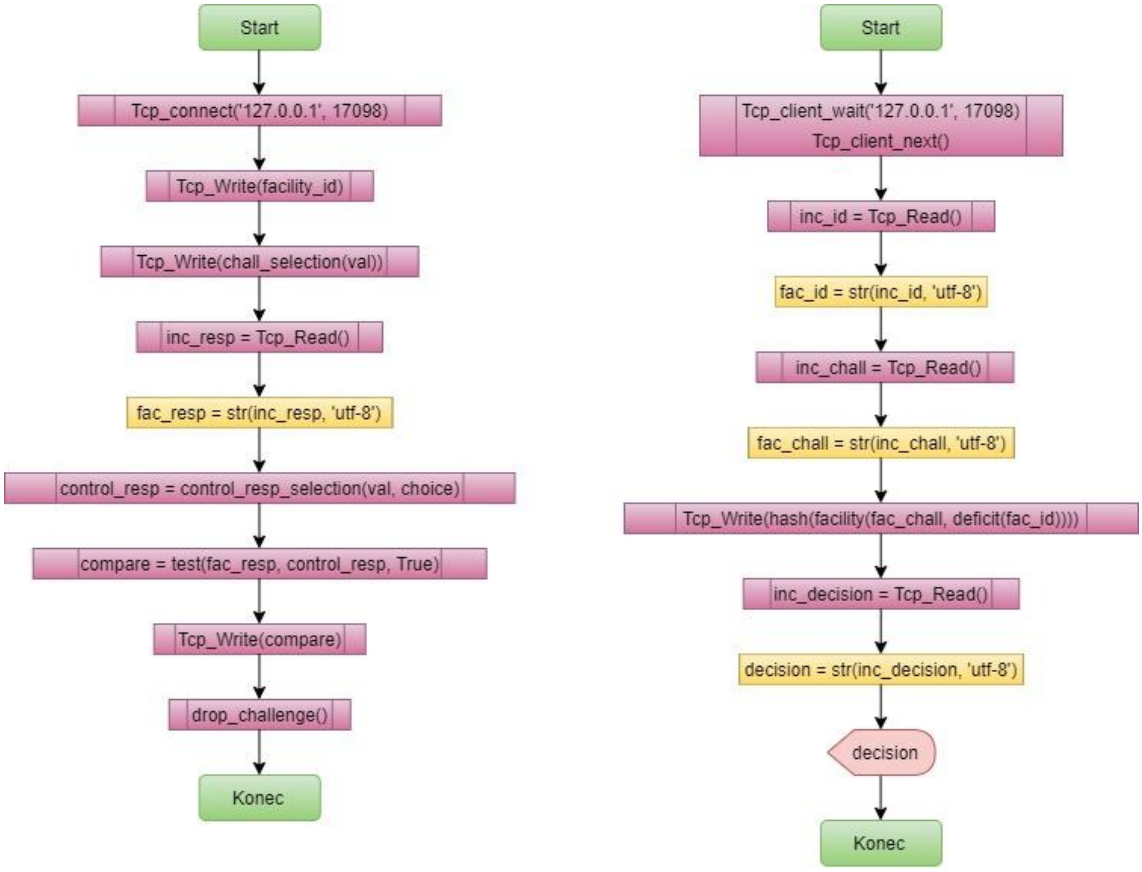
Obrázek 5.5 Vývojový diagram funkce chall_selection().

Na straně řídící jednotky je tento otisk přijat a dekódovaný uložen do proměnné fac_resp. Nyní je potřeba z databáze vyvolat odpověď příslušící danému zařízení a výzvě. K tomu slouží funkce *control_resp_selection(),* která v závislostech na hodnotách, jenž byly zvoleny na začátku autentizačního procesu (ID FNF zařízení a výzva) z databáze vybere odpovídající vzorovou odpověď a její hash uloží do proměnné control_resp.

K vyhodnocení úspěšnosti autentizace slouží funkce *test().* Tato funkce ve svých útrobách volá funkci *similar()*, jejíž vstupními hodnotami jsou proměnné obsahující nově vzniklou a referenční odpověď. Funkce tato data rozloží na jednotlivé znaky, které mezi sebou porovnává. Toto porovnání se provádí v rozmezí od prvního po předposlední znak obou odpovědí. Tato skutečnost v rámci praktického řešení této práce reprezentuje užití vzdálenostních metrik (1.2.3), jejichž užití je jednou z metod ošetření odpovědí proti nestabilitě výstupů FNF zařízení. Na základě podobnosti obou vzorů odpovědí funkce *similar()* určí, zdali se odpovědi rovnají, či naopak. Toto rozhodnutí je posléze přeneseno do funkce *test()*, která na jeho rozhodnutí zvolí, proběhla-li autentizace úspěšně, či nikoli. Rozhodnutí je poté odesláno FNF zařízení, které rozhodnutí vypíše na obrazovku.

Po úspěšné autentizaci je v rámci prevence možného útoku opakováním použitá odpověď společně se všemi odpověďmi z databáze vymazána.

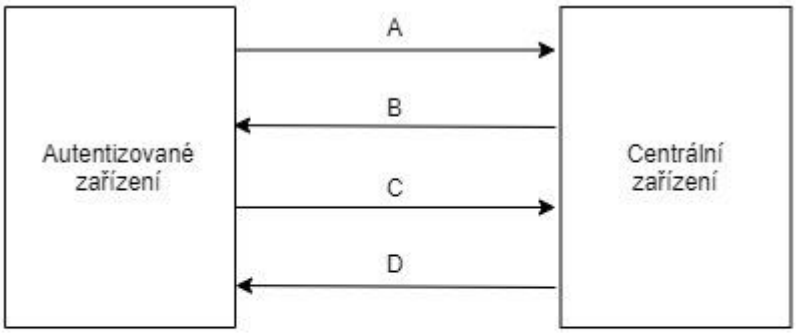
Celý průběh autentizace ze strany centrálního zařízení je graficky znázorněn na obrázku 5.7. Diagram vlevo znázorňuje stranu centrálního zařízení a diagram vpravo zastupuje stranu FNF zařízení.



Obrázek 5.6 Vývojový diagram autentizace vyžádané ze strany centrálního zařízení.

5.4.2 Autentizace ze strany FNF zařízení

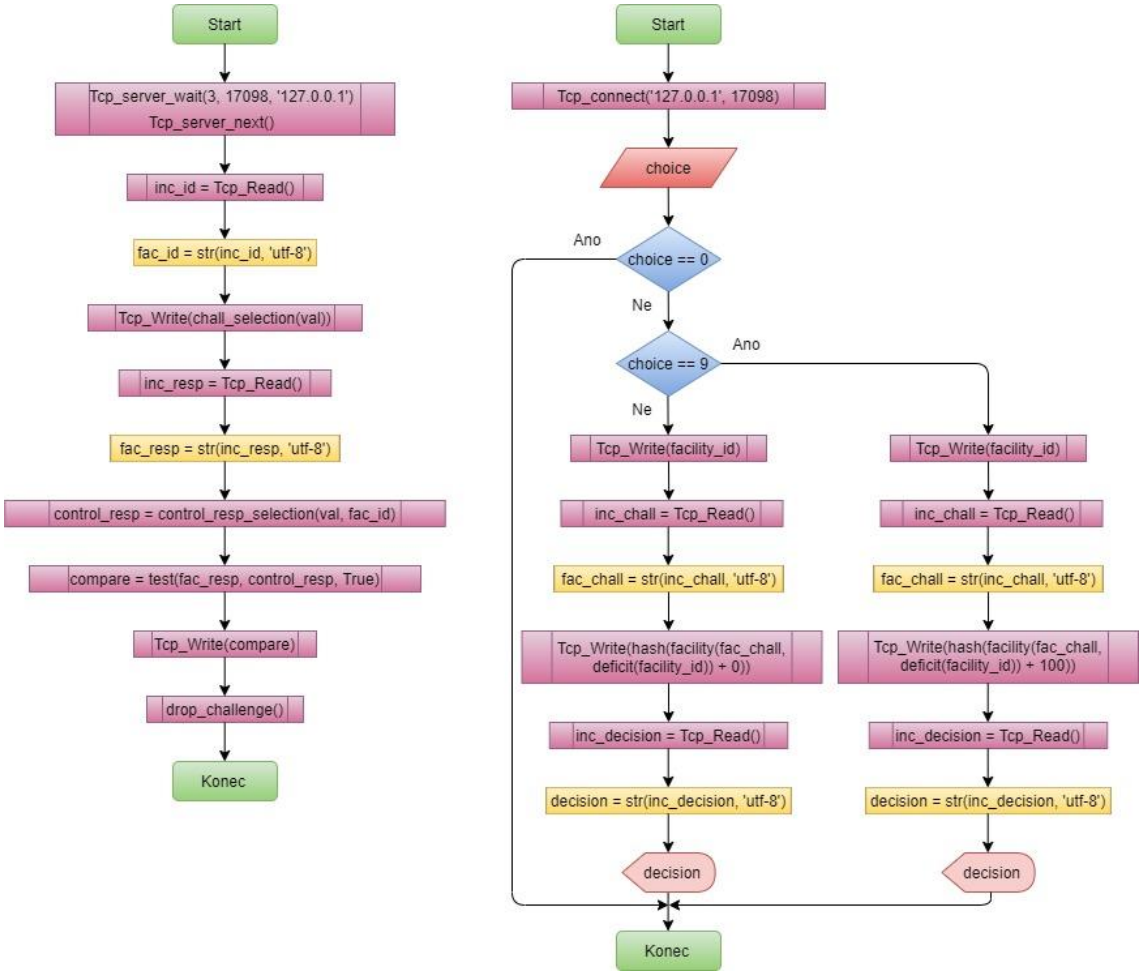
Autentizace ze strany FNF zařízení se technologicky v žádném aspektu neliší od autentizace ze strany řídící jednotky, kromě skutečnosti že strana FNF zařízení je ta, která inicializuje spojení a jako první odesílá data (identifikační číslo zařízení).



A = Žádost o autentizaci (včetně ID zařízení) X Kontrola ID v databázi
B = Výzva
C = Odpověď X Srovnání odpovědi se vzorem daného zařízení
D = Úspěšná autentizace

Obrázek 5.6 Návrh autentizace ze strany FNF zařízení.

Součástí tohoto typu autentizace je v rámci praktického řešení zaimplementována i ukázka neúspěšného ověření, kdy je k nově vzniklé výstupní hodnotě přičteno trojciferné číslo sto. Tato skutečnost naruší hodnotu odpovědi natolik, že její shoda s referenční odpovědí již nebude dostatečná a funkce *test()* vyhodnotí tento pokus o autentizaci, jako neúspěšný. Celý postup autentizace ze strany FNF zařízení je zaznamenán na diagramu 5.9.



Obrázek 5.7 Vývojový diagram autentizace ze strany FNF zařízení.

Závěr

Fyzicky neklonovatelné funkce představují velice zajímavou alternativu na poli kryptografie. Ačkoliv jsou možnosti jejich využití opravdu široké, od možné identifikace produktů až po generování šifrovací klíčů, není jejich potenciál v dnešní době na plno využit a místo nich je stále ve většině případů využíváno konvenčních kryptografických metod.

Cílem této bakalářské práce bylo seznámit případné čtenáře s principem tohoto netradičního prostředku moderní kryptografie, některými jejími zástupci napříč různými kategoriemi a v závěru nastínit jeho možné využití prostřednictvím autentizačního systému.

Co se týče samotného autentizačního systému, je zde stále prostor pro jeho případné vylepšení. Konkrétně by se mohlo jednat o vytvoření grafického rozhraní pro příjemnější uživatelský požitek a implementaci funkce zastupující vzorek protichybového kódu. Ačkoli bylo o tento poslední bod v průběhu tvorby autentizační aplikace usilováno v podobě výpočtu aritmetického průměru výstupní hodnoty FNF zařízení, jež by byla užita, jako referenční odpověď, v důsledku povahy výstupních dat bylo od této funkce upuštěno.

Komplikace ohledně samoopravného kódu nastala ve chvíli, kdy byl součet výstupních hodnot vydělen počtem opakování. Jelikož výsledek tohoto dělení byl samovolně převeden na typ float, nebyl již (z důvodu své délky až 77 znaků) po zpětném převedení na typ integer shodný s původním výstupem instance FNF. Z tohoto důvodu nebylo možné využít hodnotu po implementaci samoopravného kódu jako referenční. Vhodným kandidátem na náhradní protichybový kód by se mohl stát Grayův, popřípadě Hammingův kód, které ovšem pracují s binární podobou hodnotami. Vhodnost těchto alternativ nebyla však v rámci práce prakticky odzkoušena.

Literatura

[1] BAUDER, D. W.: An anti-counterfeiting concept for currency systems. Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990. 1983.

[2] BÖHM, Ch.; HOFER, M.: *Physical unclonable functions in theory and practice*. Springer Science & Business Media, 2012.

[3] Commission on Engineering and Technical Systems (CETS): *Counterfeit Deterrent Features for the Next-Generation Currency Design*. The National Academic Press(1993). Appendix E

[4] ČLUPEK, V.: *Autentizace s využitím lehké kryptografie*: dizertační práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2016. 114 s. Vedoucí práce byl doc. Ing. Václav Zeman, Ph.D.

[5] DEJEAN, G.; KIROVSKI, D.: RF-DNA: Radio-Frequency Certificates of*Authenticity*. In Workshop on Cryptographic Hardware and Embedded Systems –CHES 2007. Lecture Notes in Computer Science (LNCS), vol. 4727. Springer, 346–363.

[6] GASSEND, B. et al.: *Silicon physical random functions*. In Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, [2016-12-01]

[7] GASSEND, B.: *Physical random functions*. 2003, doktorská práce, Massachusetts Institute of Technology, [2019-12-11]. Dostupné z:http://csg.csail.mit.edu/pubs/memos/Memo-458/memo-458.pdf

[8] GUAJARDO, J.; KUMAR, S. S.; SCHRIJEN, G. J.; TUYLS, P.: *FPGA Intrinsic PUFs and Their Use for IP Protection*. In Workshop on Cryptographic Hardware and Embedded Systems – CHES 2007. Lecture Notes in Computer Science (LNCS), vol. 4727. Springer

[9] GUAJARDO, J. et al. Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. Information Systems Frontiers. 2009, 11.1: 19–41

[10] HEGR, V.: Fyzicky neklonovatelné funkce: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2017. 73 s. Vedoucí práce byl doc. Ing. Václav Zeman, Ph.D.

[11] HELINSKI, R.; ACHARYYA, D.; PLUSQEULLIC, J.: *A Physical Unclonable Function Defined Using Power Distribution System Equivalent Resistance Variations*. In Design Automation Conference – DAC 2009, [2019-12-11]. Dostupné z: http://ece-research.unm.edu/jimp/pubs/dac2009_PUF.pdf.

[12] INDECK, R. S. a MULLER, M. W.: *Method and apparatus for fingerprinting magnetic media*. U.S. Patent No 5,365,586, 1994.

[13] KIM, I., MAITI, A., NAZHANDALI, L., SCHAUMONT, P., VIVEKRAJA, V., ZHANG, H. 2010.: *From Statistics to Circuits: Foundations for Future Physical Unclonable Functions*. In Towards Hardware-Intrinsic Security, A.- R. Sadeghi and D. Naccache, Eds. Information Security and Cryptography. Springer, 55–78.

[14] KODÝTEK, F.: *Fyzicky neklonovatelné funkce na FPGA*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2014, [2019-12-11]. Dostupné z: https://dip.felk.cvut.cz/browse/pdfcache/kodytfil_2014bach.pdf

[15] KUMAR, S. S.; GUAJARDO, J.; MAES, R.; SCHRIJEN, G.; TUYLS, P.:*Extended Abstract: The Butterfly PUF Protecting IP on every FPGA*. 2008, [cit.2019-12-11]. Dostupné z: https://www.cosic.esat.kuleuven.be/publications/article-1154.pdf

[16] LOFSTROM, K.; DAASCH, W.R.; TAYLOR, D.: *IC identification circuit using device mismatch*. In Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International, pages 372-373, 2000.

[17] MAES, R.; VERBAUWHEDE, I.: *Physically unclonable functions: A study on the state of the art and future research directions*. In Towards Hardware-Intrinsic Security. Springer Berlin Heidelberg, 2010. p. 3–37.

[18] MAES, R.: *Physically Unclonable Functions: Constructions, Properties and Applications*. Dizertační práce. Katholieke Universiteit Leuven, 2012, [2019-12-11]. Dostupné z: https://securewww:esat:kuleuven:be/cosic/publications/thesis-211:pdf.

[19] PAPPU, R.: *Physical one-way functions*. 2001. PhD Thesis. Massachusetts Institute of Technology, [2019-12-11]. Dostupné z: http://cba.mit.edu/docs/theses/01.03.pappuphd.powf.pdf

[20] RÜHRMAIR, U. et al.: *Modeling attacks on physical unclonable functions*. In Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010. p. 237–249.

[21] SU, Y.; HOLLEMAN, J.; OTIS, B.: *A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations*. In IEEE Journal of Solid-State Circuits, 2008, [2019-12-11]. Dostupné z:https://pdfs.semanticscholar.org/72f5/c50c41e762dfcfcfa39bd19529d29f38050c.pdf

[22] SUH, G. E.; DEVADAS, S.: *Physical Unclonable Functions for Device Authentication and Secret Key Generation*. In Proceedings of the 44th annual Design Automation Conference. ACM, 2007.

[23] TOLK, K. M.: *Reflective particle technology for identification of critical components*. Sandia National Labs., Albuquerque, NM (United States), 1992.

[24] VRIJALDENHOVEN, S.: *Acoustical physical uncloneable functions*. Philips internal publication PR-TN-2004-300300. 2005, [2019-12-11]. Dostupné z: http://alexandria.tue.nl/extra1/afstversl/wsk-i/vrijaldenhoven2005.pdf

[25] YU, M.; DEVADAS, S.: *Secure and Robust Error Correction for Physical Unclonable Functions*. 2009, [2016-12-01]. Dostupné z: https://people.csail.mit.edu/devadas/pubs/secure-robust-ecc-puf.pdf

[26] SCHUSTER, D.: *Side-channel analysis of Physical Unclonable Functions (PUFs)*.Master's thesis, Technische Universität München, 2010.

[27] KODÝTEK, F.: *Behaviour Analysis and Improvement of the Proposed PUF on FPGA*. Master's thesis. Czech Technical University in Prague, Faculty ofInformation Technology, 2016, [2016-12-01]. Dostupné z:https://dspace.cvut.cz/bitstream/handle/10467/65141/F8-DP-2016-Kodytek-Filipthesis.pdf?sequence=-1&isAllowed=y

Seznam symbolů a zkratek

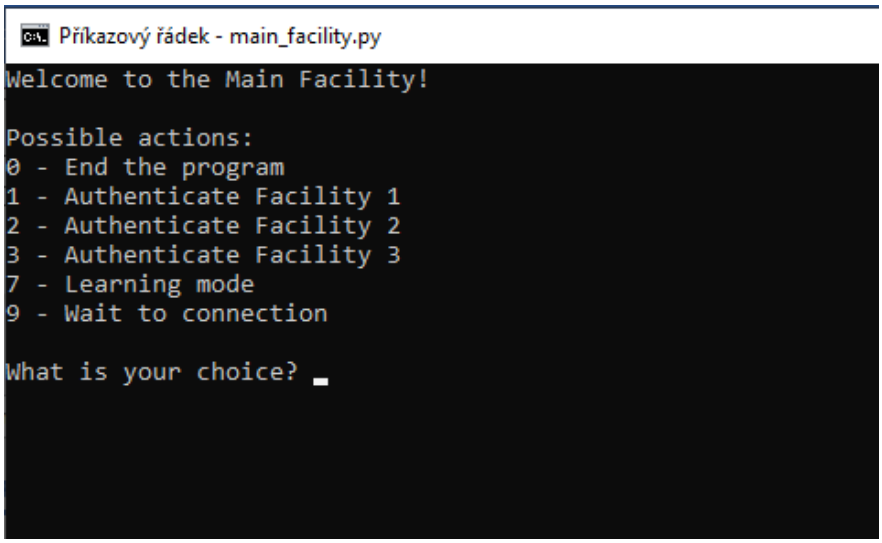
Zkratky:

CCD	Charge-Coupled Device
CD	Compact Disk
CLK	clock
CLR	clear
CZ	Centrální Zařízení
FEKT	Fakulta elektrotechniky a komunikačních technologií
FNF	Fyzicky Neklonovatelné Funkce
FPGA	Field Programmable Gate Array
ICID	Integrated Circuit IDentification
IoT	Internet of Things
LC FNF	fyzicky neklonovatelné funkce oscilačního obvodu
MITM	Man In The Middle
PRE	preset
PRF	Physical Random Function
PUF	Physical Unclonable Functions (také Physically Uncloneable Function)
RF-DNA FNF	Radio-Frequency DNA fyzicky neklonovatelné funkce
RFID	Radio Frequency IDentification
SRAM	Static Random Access Memory
VUT	Vysoké učení technické v Brně

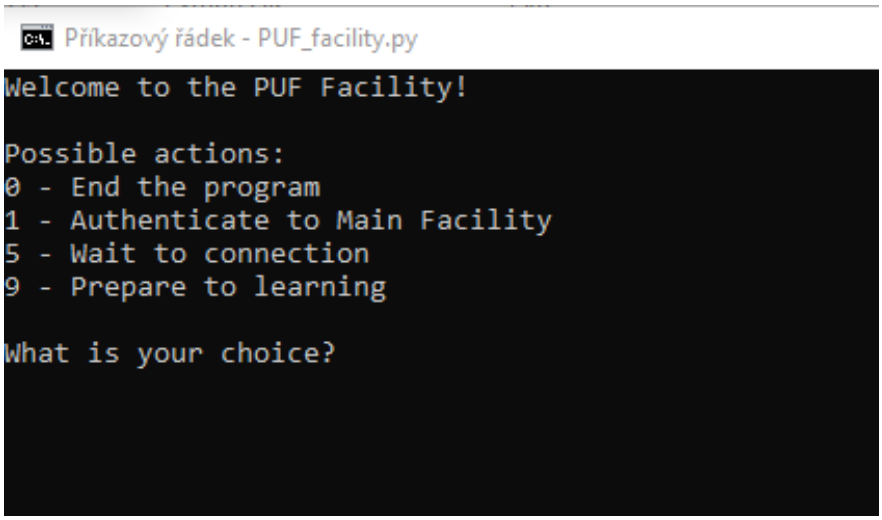
Seznam příloh

Příloha A – Popis činnosti autentizační aplikace

Po spuštění obou programů autentizační aplikace se na obou stranách zobrazí kontextové menu (obrázek 0.1 a 0.2), které uživatele přivítá a vybídne jej k další akci. Tyto akce je možné provádět na obou stranách aplikace. Uživatel si jen musí uvědomit, kterou z akcí chce provést a pak jen stačí následovat níže uvedené instrukce.



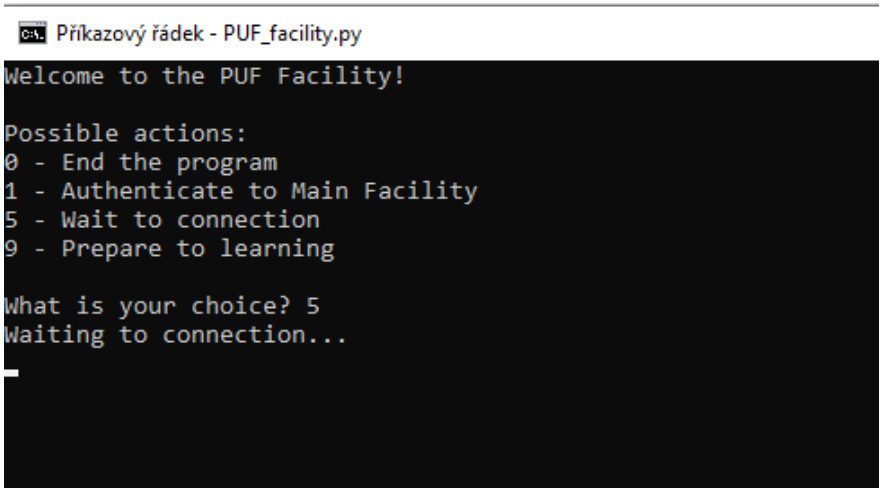
Obrázek 0.2 Kontextové menu Centrálního zařízení.



Obrázek 0.1 Kontextové menu zařízení FNF.

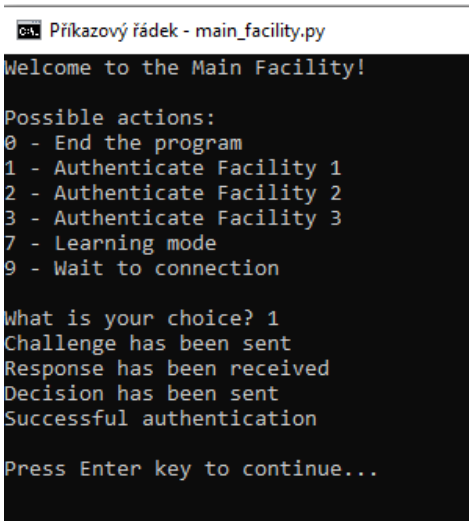
Žádost o autentizaci ze strany centrálního zařízení:

Chceme-li provést autentizaci jednoho ze tří FNF zařízení ze strany řídící jednotky, je ze všeho nejdříve nutné spustit na straně FNF zařízení komunikační kanál, ke kterému se bude centrální zařízení připojovat. To provedeme stisknutím klávesy 5 (viz obrázek 0.3).

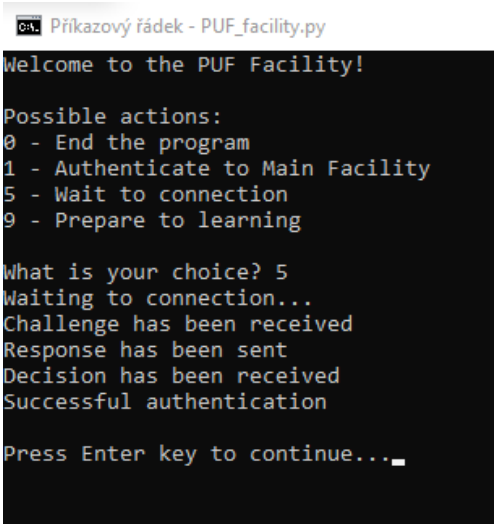


Obrázek 0.3 FNF zařízení otevřelo komunikační kanál a nyní čeká na žádost o autentizaci.

Nyní si na straně centrálního zařízení vybereme, po kterém FNF zařízení budeme žádat autentizaci. Stiskneme příslušnou klávesu (1-3) a ověřovací fáze započne. Vnitřní procesy autentizace ze strany centrálního zařízení jsou popsány v kapitole 5.4.1. Průběh autentizace je znázorněn na obrázku 0.4 a 0.5. Tento postup je shodný pro autentizaci všech FNF zařízení. Poté, co proběhne autentizace stiskneme klávesu Enter, což nás vrátí do hlavního menu aplikace.



Obrázek 0.4 Průběh autentizace na straně CZ.

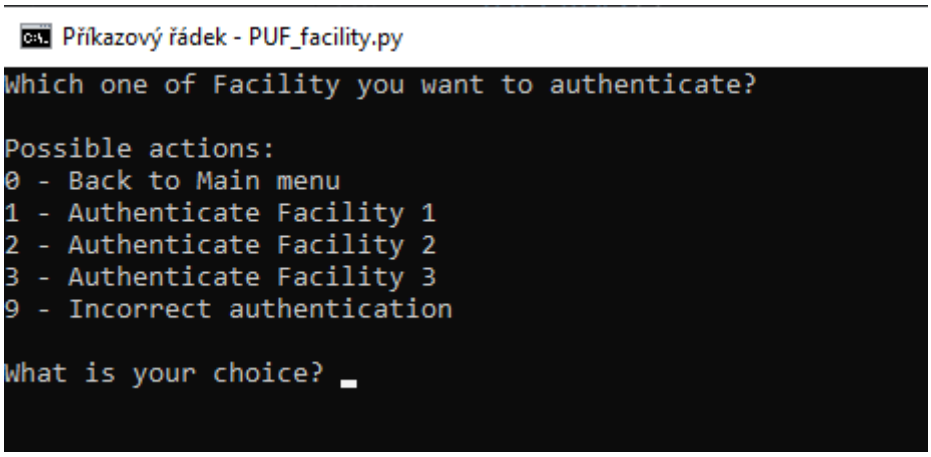


Obrázek 0.5 Průběh autentizace na straně FNF zařízení.

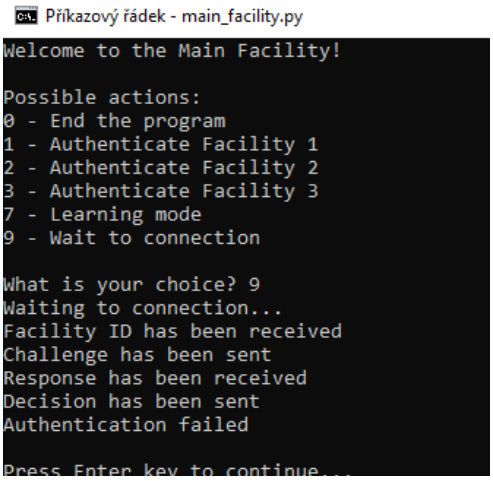
Žádost o autentizaci ze strany FNF zařízení:

Chceme-li provést autentizaci ze strany FNF zařízení, je nutné nejdříve spustit na straně centrálního zařízení komunikační kanál, ke kterému se bude FNF zařízení připojovat. Stiskneme tedy klávesu 9 a na obrazovce se nám zobrazí analogický výjev, jako na obrázku 0.3. Nyní když máme stranu centrálního zařízení připravenou je nutné na straně FNF zařízení vybrat příkaz pro autentizaci. Ten se skrývá pod klávesou 1.

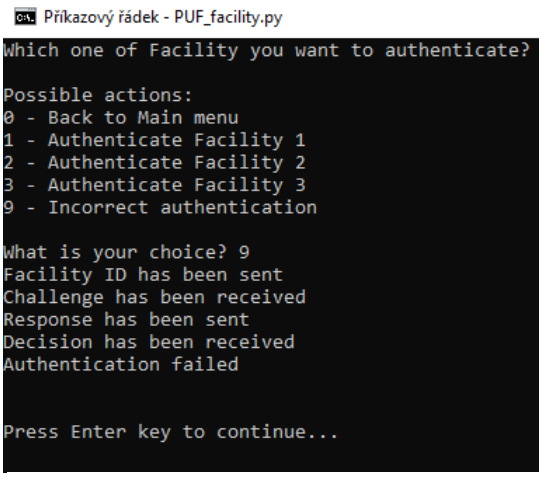
Po stisknutí tohoto tlačítka se zobrazí druhé kontextové menu (obrázek 0.6), kde máme na výběr autentizaci zařízení 1-3, ukázku chybné autentizace (pod klávesou 9) anebo možnost návratu zpět do hlavního meny. Pro jednu ze čtyř ukázek autentizace zvolíme klávesy 1-3 nebo 9. Zvolíme-li možnost 1-3, bude výjev na obrazovce obdobný obrázkům 0.4 a 0.5. Z toho důvodu je v rámci této dokumentace zvolena možnost chybného ověření (obrázky 0.7 a 0.8).



Obrázek 0.6 Kontextové menu pro autentizaci ze strany FNF zařízení.



Obrázek 0.7 Chybné ověření na straně CZ.

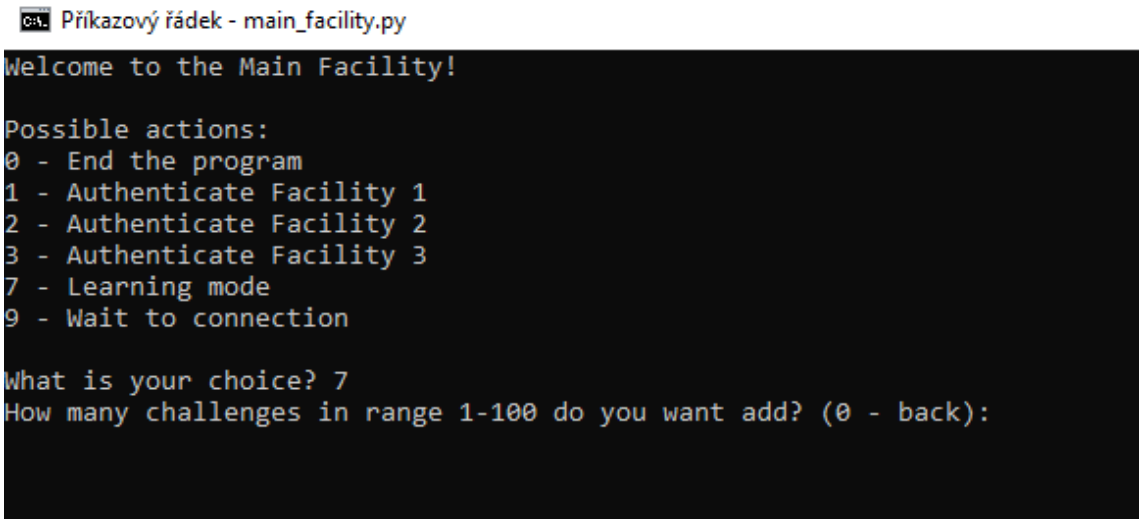


Obrázek 0.8 Chybné ověření na straně FNF zařízení.

Inicializační fáze systému:

Aplikace rovněž obsahuje možnost spuštění inicializační fáze (podrobný rozbor této funkce se nachází v kapitole 5.3). Chceme-li využít této možnosti k naplnění databáze, je nejdříve nutné vybrat z hlavního menu na straně FNF zařízení možnost „Prepare to learning“, čímž otevřeme komunikační kanál určený pro inicializaci. Tak učiníme stisknutím klávesy 9 (výjev na obrazovce bude analogický obrázku 0.3).

Nyní na straně centrálního zařízení zvolíme klávesou 7, volbu pro naplnění databáze. Po stisknutí klávesy se nás aplikace dotáže, kolik výzev v rozmezí 1-100 chceme do databáze vložit (viz obrázek 0.9). Výběr zadáváme numericky a potvrdíme stisknutím klávesy Enter. Nyní probíhá plnění databáze výzva – odpověď (obrázek 0.10 a 0.11)



Obrázek 0.9 Dotaz na množství výzev.

.

Příkazový řádek - main_facility.py

```
Welcome to the Main Facility!

Possible actions:
0 - End the program
1 - Authenticate Facility 1
2 - Authenticate Facility 2
3 - Authenticate Facility 3
7 - Learning mode
9 - Wait to connection

What is your choice? 7
How many challenges in range 1-100 do you want add? (0 - back): 3
Challenge has been sent
Response of Facility 1 has been received
Response of Facility 2 has been received
Response of Facility 3 has been received
Upload to database completed successfully.
Challenge has been sent
Response of Facility 1 has been received
Response of Facility 2 has been received
Response of Facility 3 has been received
Upload to database completed successfully.
Challenge has been sent
Response of Facility 1 has been received
Response of Facility 2 has been received
Response of Facility 3 has been received
Upload to database completed successfully.

Press Enter key to continue...
```

Obrázek 0.11 Plnění databáze na straně centrálního zařízení.

Příkazový řádek - PUF_facility.py

```
Welcome to the PUF Facility!

Possible actions:
0 - End the program
1 - Authenticate to Main Facility
5 - Wait to connection
9 - Prepare to learning

What is your choice? 9
Waiting to connection...
Challenge has been received
Challenge has been received
Challenge has been received
Responses have been sent

Press Enter key to continue...
```

Obrázek 0.10 Plnění databáze na straně FNF zařízení.